Wspólna opinia EROD-EIOD nr 02/2023 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia cyfrowego euro

Przyjęta 17 października 2023 r.

SPIS TREŚCI

1 Kontekst 5
2 Zakres opinii 8
3 Uwagi ogólne 10
4 Rozdział i – przedmiot i definicje 13
5 Rozdział III – prawny środek płatniczy 15
6 Rozdział IV – dystrybucja 15
7 Rozdział V – korzystanie z cyfrowego euro jako środka przechowywania wartości i jako środka płatniczego 17
8 Rozdział VII – cechy techniczne 18
8.1 Formy obsługi cyfrowego euro w trybie offline i online 18
8.2 Warunkowe transakcje płatnicze w cyfrowym euro 19
8.3 Europejskie portfele tożsamości cyfrowej 20
8.4 Rozliczenie 21
8.5 Ogólny mechanizm wykrywania oszustw i zapobiegania im 21
9 Bezpieczeństwo cybernetyczne i odporność operacyjna 24
10 Rozdział VIII – prywatność i ochrona danych 25
10.1 Artykuł 34: Przetwarzanie przez dostawców usług płatniczych 25
10.2 Artykuł 35: Przetwarzanie danych osobowych przez EBC lub krajowe banki centralne 29
10.3 Artykuł 36: Przetwarzanie przez dostawców usług wsparcia 30
11 Rozdział IX – Przeciwdziałanie praniu pieniędzy 32
12 Rozdział X – Przepisy końcowe 36

Streszczenie

Dwa lata po rozpoczęciu etapu badania dotyczącego emisji cyfrowego euro przez Europejski Bank Centralny (EBC) Parlament Europejski i Rada Unii Europejskiej przeanalizują w nadchodzących miesiącach wniosek dotyczący rozporządzenia ustanawiającego cyfrowe euro jako cyfrową walutę banku centralnego. Mając na uwadze szczególne znaczenie cyfrowego euro dla podstawowych praw do prywatności i ochrony danych osobowych, Komisja Europejska zwróciła się do EROD i EIOD o wydanie wspólnej opinii w sprawie tego wniosku.

W ujęciu ogólnym, przypominając, że wartość dodana cyfrowego euro na wysoce konkurencyjnym rynku płatności wynikałaby głównie z jego poufności, EROD i EIOD z dużym zadowoleniem przyjmują fakt, że użytkownicy technologii cyfrowych zawsze będą mogli wykonywać płatności w cyfrowym euro lub gotówce, a także że cyfrowe euro nie będzie „pieniądzem programowalnym". W niniejszej wspólnej opinii z zadowoleniem przyjmuje się również fakt, że wniosek ma służyć zapewnieniu wysokiego poziomu prywatności i ochrony danych w odniesieniu do cyfrowego euro, a także uznaje się wysiłki podjęte w tym celu we wniosku, w szczególności wprowadzenie „trybu offline", wysiłki podjęte w celu zminimalizowania przetwarzania danych osobowych związanych z cyfrowym euro oraz w celu uwzględnienia ochrony danych w fazie projektowania i uwzględnienia domyślnej ochrony danych.

EROD i EIOD, kierując się podejściem „uwzględniania prywatności i ochrony danych w fazie projektowania", zwracają jednak uwagę współprawodawców na szereg obaw związanych z ochroną danych osobowych, które to obawy, jeśli nie zostaną uwzględnione we wniosku, mogą podważyć zaufanie obywateli do przyszłego cyfrowego euro, a tym samym jego społeczną absorpcję. W związku z tym EROD i EIOD rozwijają w niniejszej opinii swoje stanowiska przyjmowane już od 2021 r.

Po pierwsze, chociaż EROD i EIOD z zadowoleniem przyjmują fakt, że dystrybucja cyfrowego euro byłaby prowadzona w sposób „zdecentralizowany", tj. przez pośredników finansowych, a nie bezpośrednio przez Eurosystem, uważają, że w tekście legislacyjnym należy zawrzeć dalsze wyjaśnienia dotyczące sposobów dystrybucji cyfrowego euro.

Ponadto EROD i EIOD uważają, że należy przedstawić więcej wyjaśnień dotyczących konieczności i proporcjonalności pojedynczego punktu dostępu służącego do weryfikacji unikatowych identyfikatorów cyfrowego euro, a także sposobu, w jaki ochrona danych w fazie projektowania i domyślna ochrona danych mają być wdrażane w tym zakresie. Dodatkowo tekst legislacyjny powinien zawierać wyjaśnienia dotyczące sposobu, w jaki dane osobowe musiałyby być przetwarzane przez dostawców usług płatniczych w celu egzekwowania w praktyce limitów utrzymywanej kwoty. Apeluje się również o większą jasność w odniesieniu do przetwarzania danych osobowych w celu egzekwowania limitów opłat ewentualnie pobieranych przez dostawców usług płatniczych.

W odniesieniu do infrastruktury rozrachunkowej, którą EBC ma zapewnić i którą ma zarządzać, EROD i EIOD są zdania, że część normatywna wniosku powinna zawierać wiążący obowiązek zapewniający pseudonimizację wszystkich danych dotyczących transakcji względem EBC i krajowych banków centralnych.

Co ważne, EROD i EIOD uważają również, że przepisy dotyczące ogólnego mechanizmu wykrywania oszustw i zapobiegania im (FDPM), który EBC może ustanowić w celu ułatwienia dostawcom usług płatniczych wykrywania oszustw i zapobiegania im, nie są przewidywalne, co podważa pewność prawa i zdolność do oceny konieczności ustanowienia takiego mechanizmu. Nie jest jasne w szczególności, które zadania byłyby wykonywane przez EBC (w roli ewentualnych organów nadzorujących zwalczanie oszustw prowadzone przez dostawców usług płatniczych) z jednej strony, a które zadania (i związane z nimi przetwarzanie danych) byłyby wykonywane przez dostawców usług płatniczych z drugiej strony. Współprawodawców wzywa się zatem, aby dokładniej wykazali konieczność istnienia takiego mechanizmu oraz określili jasne i precyzyjne zasady regulujące zakres i stosowanie przewidywanego FDPM, w tym w odniesieniu do charakteru wsparcia udzielanego przez EBC dostawcom usług

płatniczych. Jeżeli takiej konieczności nie można wykazać, EROD i EIOD zalecają wprowadzenie mniej inwazyjnych środków z punktu widzenia ochrony danych, wraz z wdrożeniem odpowiednich zabezpieczeń.

Ponadto EROD i EIOD wskazują w niniejszej wspólnej opinii na potencjalne zagrożenia, na jakie cyfrowe euro mogłoby być narażone z punktu widzenia IT i cyberbezpieczeństwa, i zalecają umieszczenie w preambule wniosku wyraźnego odniesienia do obowiązujących ram prawnych w zakresie cyberbezpieczeństwa.

Jeśli chodzi o aspekty cyfrowego euro związane z prywatnością i ochroną danych, EIOD i EROD z aprobatą odnotowują starania podjęte w rozdziale VIII i odpowiednich załącznikach w celu określenia celów i kategorii danych osobowych do przetwarzania przez każdy z podmiotów zaangażowanych w emisję i wykorzystanie cyfrowego euro. Współprawodawcy powinni jednak przedstawić dalsze wyjaśnienia dotyczące w szczególności podstaw prawnych mających zastosowanie do tych operacji przetwarzania, podziału obowiązków, jak również rodzajów danych osobowych, które mają być przetwarzane przez każdy z tych podmiotów.

Wreszcie EROD i EIOD ubolewają nad faktem, że we wniosku odrzucono przyjęcie podejścia polegającego na „selektywnej ochronie prywatności" w odniesieniu do płatności o niskiej wartości dokonywanych w trybie online. W tym względzie należy zauważyć, że poziom ryzyka związanego z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu w odniesieniu do cyfrowego euro w trybie online będzie zależał od zastosowanych technologii i wyborów projektowych dokonanych w fazie koncepcyjnej. Biorąc pod uwagę możliwe środki łagodzące, które można wdrożyć w celu zmniejszenia takiego ryzyka, EROD i EIOD zdecydowanie zalecają współprawodawcom rozszerzenie szczególnego systemu mającego zastosowanie do trybu offline na tryb online dla transakcji o niskiej wartości, z progiem, poniżej którego nie byłoby śledzenia transakcji na potrzeby przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

Zważywszy że prace EBC nad cyfrowym euro trwają równolegle z pracami współprawodawców, EROD i EIOD przypominają o obowiązku przeprowadzania oceny skutków dla ochrony danych przez wszystkich administratorów i współadministratorów danych związanych z cyfrowym euro w zakresie, w jakim spełnione są wymogi art. 35 RODO lub art. 39 EUDPR. Ponadto we wniosku należy przypomnieć o obowiązku uwzględnienia prywatności i ochrony danych już w fazie projektowania oraz uwzględnienia domyślnej ochrony danych przy ustalaniu projektu operacyjnego i dokonywaniu wyborów technologicznych.

Po przyjęciu przepisów dotyczących cyfrowego euro EROD i EIOD, każde w ramach swoich odpowiednich obowiązków, będą nadal monitorować jego wdrażanie i będą gotowe udzielać współprawodawcom i EBC wskazówek dotyczących aspektów ochrony danych osobowych związanych z cyfrowym euro.

Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych

uwzględniając art. 42 ust. 2 rozporządzenia 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 („EUDPR")[1],

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[2],

uwzględniając wniosek Komisji Europejskiej z dnia 29 czerwca 2023 r. o wydanie wspólnej opinii Europejskiej Rady Ochrony Danych i Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia w sprawie ustanowienia cyfrowego euro[3] oraz wniosku dotyczącego rozporządzenia w sprawie świadczenia usług związanych z cyfrowym euro przez dostawców usług płatniczych zarejestrowanych w państwach członkowskich, których walutą nie jest euro, oraz zmieniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1230[4],

PRZYJMUJĄ NINIEJSZĄ WSPÓLNĄ OPINIĘ

1 KONTEKST

1. 28 czerwca 2023 r. Komisja Europejska przyjęła pakiet legislacyjny[5] dotyczący cyfrowego euro, obejmujący wniosek ustanawiający ramy prawne dla ewentualnego cyfrowego euro[6]. Wniosek ten ma na celu ustanowienie i uregulowanie podstawowych aspektów cyfrowego euro, którego emisja jest prerogatywą Europejskiego Banku Centralnego (zwanego dalej „EBC"). Projekt cyfrowego euro rozpoczął się przed przyjęciem pakietu legislacyjnego dotyczącego cyfrowego euro. Poniżej EROD i EIOD przywołują chronologię kluczowych wydarzeń, które doprowadziły do przyjęcia pakietu legislacyjnego dotyczącego cyfrowego euro, w tym opinie wyrażone przez EROD w tej sprawie.

2. W październiku 2020 r., w kontekście rosnącego na całym świecie zainteresowania walutami cyfrowymi banków centralnych, EBC rozpoczął konsultacje publiczne w sprawie ewentualnego cyfrowego euro, nowej formy cyfrowej waluty banku centralnego do użytku w płatnościach

[1] Dz.U. L 295 z 21.11.2018, s. 39.
[2] Odniesienia do „państw członkowskich" w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[3] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia cyfrowego euro, COM/2023/369 final.
[4] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie świadczenia usług związanych z cyfrowym euro przez dostawców usług płatniczych zarejestrowanych w państwach członkowskich, których walutą nie jest euro, oraz zmieniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1230, COM/2023/368 final.
[5] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3501
[6] Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO i RADY w sprawie ustanowienia cyfrowego euro (COM/2023/369 final)

detalicznych, która ma na celu uzupełnienie fizycznego pieniądza euro[7]. Cele polityczne ustanowienia cyfrowego euro to zapewnienie obywatelom UE stałego dostępu do waluty banku centralnego w kontekście malejącego wykorzystania fizycznych środków pieniężnych, wspieranie włączenia finansowego, a także propagowanie innowacji i strategicznej autonomii UE w odniesieniu do płatności. W kwietniu 2021 r. EBC opublikował sprawozdanie dotyczące informacji zwrotnych przekazanych podczas konsultacji publicznych[8]. Ze sprawozdania wynika, że 43% respondentów, zarówno obywateli, jak i przedsiębiorstw, za najważniejszą cechę cyfrowego euro uznało poufność.

3. 18 czerwca 2021 r. EROD wysłała pismo do instytucji europejskich w sprawie aspektów prywatności i ochrony danych związanych z ewentualnym wprowadzeniem cyfrowego euro[9]. W piśmie tym EROD podkreśliła potrzebę, aby instytucje europejskie pracowały nad cyfrowym euro, które w pełni uwzględniałoby „prywatność i ochronę danych już w fazie projektowania i domyślną ochronę danych", zgodnie z wynikami konsultacji publicznych rozpoczętych przez EBC rok wcześniej. Ponadto EROD zwróciła uwagę na zagrożenia dla prywatności oraz podstawowych praw i wolności związane z takim projektem, jeżeli cyfrowe euro nie zostanie odpowiednio zaprojektowane. W szczególności EROD podkreśliła ryzyko ogólnego śledzenia transakcji w całej infrastrukturze płatniczej, ryzyko nadmiernej identyfikacji obywateli korzystających z cyfrowego euro, ryzyko dla bezpieczeństwa danych dotyczących płatności oraz zaoferowała pomoc EROD w ograniczeniu tych rodzajów ryzyka. Co więcej, w piśmie opowiedziano się za możliwością anonimizacji części transakcji lub co najmniej za wysokim poziomem pseudonimizacji. Wreszcie EROD wskazała, że fizyczne środki pieniężne są odpowiednim punktem odniesienia dla projektu cyfrowego euro, zwłaszcza w celu znalezienia właściwej równowagi między ochroną prywatności i ochroną danych z jednej strony, a przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu z drugiej strony.

4. 14 lipca 2021 r. EBC rozpoczął etap badania dotyczący projektu cyfrowego euro. Ten 24-miesięczny etap miał na celu zajęcie się kluczowymi kwestiami dotyczącymi projektowania i dystrybucji cyfrowej formy euro, a także ocenę ewentualnego wpływu cyfrowego euro na rynek. Kolejnym celem było zidentyfikowanie opcji projektowych, tak aby zapewnić prywatność i uniknąć ryzyka dla obywateli strefy euro, pośredników i całej gospodarki. W ramach pomocy udzielanej instytucjom europejskim w tym zakresie EROD wzięła udział w procesie konsultacji na etapie badania i odbyła kilka spotkań z ekspertami EBC. Oprócz stanowisk wyrażanych publicznie, EROD organizowała regularne wewnętrzne spotkania na ten temat, w których uczestniczyli eksperci Komisji. Komisja miała zatem możliwość skorzystania z regularnych nieformalnych porad EROD na etapie opracowywania przedmiotowego wniosku.

---

[7] EBC, *Report on a digital euro* (Sprawozdanie w sprawie cyfrowego euro), październik 2020 r., dokument dostępny pod adresem: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

[8] EBC, *Report on the public consultation on a digital euro* (Sprawozdanie z konsultacji publicznych w sprawie cyfrowego euro), kwiecień 2021 r., dokument dostępny pod adresem: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html

[9] EROD, pismo do instytucji europejskich w sprawie aspektów prywatności i ochrony danych związanych z ewentualnym wprowadzeniem cyfrowego euro, 18 czerwca 2021 r., dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2021-07/edpb_letter_out_2021_0111-digitaleuro-toecb_en_1.pdf

5. W kwietniu 2022 r. Komisja rozpoczęła ukierunkowane konsultacje publiczne[10] w celu zebrania dalszych informacji na temat szeregu aspektów, w tym potrzeb i oczekiwań użytkowników, spodziewanego wpływu na kluczowe gałęzie przemysłu, a także na prywatność i ochronę danych. EROD odpowiedziała na te konsultacje w czerwcu 2022 r[11]. W swojej odpowiedzi EROD przypomniała o swoim stanowisku na rzecz całkowitego braku kontroli w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu poniżej pewnego progu dla transakcji o niskiej wartości oraz o konieczności unikania centralizacji transakcji przez jakikolwiek podmiot publiczny lub prywatny, opowiadając się za lokalnym przetwarzaniem i przechowywaniem danych dotyczących transakcji pod kontrolą użytkownika. Ponadto EROD podkreśliła, że należy unikać jakiegokolwiek dostępu do danych dotyczących transakcji przez EBC i krajowe banki centralne (zwane dalej „Eurosystemem") w celu ograniczania oszustw lub egzekwowania przepisów podatkowych. Wreszcie EROD wskazała, że wprowadzenie limitów utrzymywanej kwoty lub progów opłat miałoby wpływ na prawa i wolności osób, których dane dotyczą, ponieważ wymagałoby to dodatkowych zbiorów danych i kontroli.

6. We wrześniu 2022 r. EBC opublikował pierwsze sprawozdanie z postępów na etapie badania i zaproponował w tym sprawozdaniu kilka wariantów ochrony danych i projektowania prywatności dla cyfrowego euro. EBC przypomniał również, że ramy regulacyjne ustanowione przez współprawodawców będą kluczowe w odniesieniu do aspektów prywatności cyfrowego euro[12]. W szczególności EBC zaproponował scenariusz bazowy oparty na rozwoju cyfrowego euro dostępnego w trybie online, w którym wszystkie transakcje są zatwierdzane przez pośredników finansowych dystrybuujących cyfrowe euro i które są dla nich w pełni przejrzyste od pierwszej emisji cyfrowego euro. Dwa warianty: „selektywna ochrona prywatności", w której wyższy stopień prywatności byłby zapewniony dla płatności w trybie online o niskiej wartości / niskim ryzyku, oraz „funkcjonalność w trybie offline", w przypadku której śledzenie nie miałoby miejsca dla płatności w trybie offline o niskiej wartości wykonywanych w bliskiej odległości fizycznej, zostały opisane przez EBC jako „wykraczające poza poziom podstawowy" i podlegające dalszemu badaniu przez współprawodawców.

7. 10 października 2022 r. EROD opublikowała oświadczenie[13] przypominające o konieczności unikania systematycznego śledzenia transakcji w takiej architekturze opartej na kontach. Ostrzegła, że zatwierdzanie wszystkich transakcji z użyciem cyfrowego euro może nie być zgodne z pojęciem konieczności i proporcjonalności ochrony danych, zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „TSUE"). EROD przypomniała, że wprowadzenie progu prywatności dla transakcji o niskiej wartości, poniżej którego nie powinno występować śledzenie transakcji, było konieczne, aby zrównoważyć ryzyko, zarówno

[10] https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-digital-euro_en

[11] EROD, odpowiedź na ukierunkowane konsultacje Komisji Europejskiej w sprawie cyfrowego euro, przyjęta 14 czerwca 2022 r., dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2022-06/edpb_responseconsultation_20220614_digitaleuro_en.pdf

[12] EBC, *Progress on the investigation phase of a digital euro* (Postępy na etapie badania cyfrowego euro), 29 września 2022 r., dokument dostępny pod adresem: https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf?8eec0678b57e98372a7ae6b59047604b

[13] Oświadczenie EROD 04/2022 w sprawie wyborów projektowych dotyczących cyfrowego euro z perspektywy prywatności i ochrony danych, przyjęte 10 października 2022 r., dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf

w przypadku trybu online, jak i w przypadku trybu offline. Ponadto EROD wezwała do przeprowadzenia publicznej i demokratycznej debaty na ten temat.

8. Jeśli chodzi o system przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w odniesieniu do cyfrowego euro, EROD wskazała, że obecne ramy prawne dotyczące płatności elektronicznych nie wydają się odpowiednie dla narzędzia takiego jak cyfrowe euro, które ma zasadniczo odmienne cechy pod względem celów polityki, a także biorąc pod uwagę poziom zaufania niezbędny do spełnienia oczekiwań wyrażonych podczas konsultacji publicznych[14]. W związku z tym EROD opowiedziała się za utworzeniem specjalnego systemu prawnego dla cyfrowego euro i zaleciła przeprowadzenie oceny ryzyka zarówno dla prywatności, jak i dla przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w tym samym czasie.

9. EROD i EIOD ponownie wskazują, że wartość dodana cyfrowego euro, na i tak już wysoce konkurencyjnym europejskim rynku płatności, polegałaby głównie na jego cechach zapewniających prywatność i ochronę danych. Według EROD i EIOD cechy cyfrowego euro zapewniające prywatność i ochronę danych są rzeczywiście warunkiem wstępnym zdobycia zaufania społeczeństwa do cyfrowej formy waluty banku centralnego, a także decydującym czynnikiem wpływającym na jej przyjęcie przez obywateli UE[15]. Zaufania tego nie powinny podważać nieodpowiednie zaprojektowanie cyfrowego euro lub nieodpowiednie ramy prawne. Uniknięcie takiej sytuacji jest właśnie celem wspólnej opinii.

2 ZAKRES OPINII

10. 29 czerwca 2023 r. Komisja zwróciła się do EROD i EIOD o wydanie wspólnej opinii (zwanej dalej „opinią") zgodnie z art. 42 ust. 2 rozporządzenia (UE) 2018/1725 (zwanego dalej „EUDPR") w sprawie dwóch wniosków dotyczących rozporządzeń stanowiących część „pakietu jednowalutowego". Ten pakiet legislacyjny obejmuje:

- wniosek dotyczący rozporządzenia w sprawie ustanowienia cyfrowego euro[16] (zwany dalej „wnioskiem");
- wniosek dotyczący rozporządzenia w sprawie świadczenia usług związanych z cyfrowym euro przez dostawców usług płatniczych zarejestrowanych w państwach członkowskich, których

[14] Zob. pkt 2 powyżej i przypis 8.

[15] W tym względzie EROD i EIOD zauważają, że zgodnie z sondażem przeprowadzonym w imieniu Bundesbanku w Niemczech głównymi możliwymi przeszkodami dla respondentów były: brak wartości dodanej (w przypadku 77% respondentów), strach przed pierwszym krokiem w kierunku zniesienia fizycznych środków pieniężnych (61%) oraz możliwość ogólnego nadzoru nad zwyczajami nabywczymi (54%) (Deutsche Bundesbank, sprawozdanie miesięczne, październik 2021 r., dostępne na stronie internetowej: https://www.bundesbank.de/resource/blob/879312/8070 18037068359550e1d89a5dc366fe/mL/2021-10-digitaler-euro-private-haushalte-data.pdf). Ponadto, jak wynika z ostatniego badania „SPACE" EBC, 60% obywateli strefy euro uważa, że ważne jest, aby możliwe było wykonanie płatności gotówką. Postrzegane kluczowe zalety gotówki to dla nich anonimowość i ochrona prywatności (EBC, Badanie dotyczące postaw płatniczych konsumentów w strefie euro, 20 grudnia 2022 r., dostępne na stronie internetowej: https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ ecb.spacereport202212~783ffdf46e.en.html).

[16] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia cyfrowego euro, COM/2023/369 final.

walutą nie jest euro, oraz zmieniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1230[17].

11. Te dwa wnioski, które sprzyjają sobie nawzajem, mają na celu ustanowienie cyfrowego euro i zapewnienie Europejczykom zarówno gotówkowych, jak i cyfrowych możliwości płatności, gdy chcą płacić pieniędzmi banku centralnego. W kontekście niniejszej opinii sformułowano jedynie zalecenia w odniesieniu do wniosku dotyczącego rozporządzenia w sprawie ustanowienia cyfrowego euro.

12. Wniosek zapewnia ramy prawne dla przyjęcia i emisji cyfrowego euro przez EBC i w tym celu w dużej mierze opiera się na podejściu zawartym w trzecim sprawozdaniu z postępów wydanym przez EBC w kwietniu 2023 r[18].

13. Dokładniej rzecz ujmując, we wniosku ustanawia się ramy emisji cyfrowego euro przez EBC zgodnie z wnioskiem i bez uszczerbku dla niezależnego stanowiska i uprawnień EBC wynikających z Traktatów[19]. Ponadto we wniosku ustanawia się cyfrowe euro jako prawny środek płatniczy i ustala się zasady jego dystrybucji za pośrednictwem dostawców usług płatniczych. Co więcej, wniosek określa role i obowiązki krajowych banków centralnych i EBC w zakresie emisji i nadzoru finansowego oraz przewiduje podstawy charakterystyki technicznej cyfrowego euro. Po przyjęciu wniosku, o którym mowa, EBC musiałby dalej rozwijać normy techniczne na potrzeby wdrożenia cyfrowego euro.

14. We wniosku proponuje się dwa rodzaje cyfrowego euro: tryb online i offline. Wybór każdego z tych trybów przez użytkownika cyfrowego euro ma istotne skutki dla ochrony danych, ponieważ we wniosku rozróżnia się obowiązki między tymi trybami, biorąc pod uwagę na przykład rozliczanie transakcji i stosowanie przepisów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu[20].

15. Wniosek ma istotny wpływ na podstawowe prawa osób fizycznych do prywatności i ochrony danych osobowych. Za nadzór nad przetwarzaniem danych osobowych na podstawie wniosku będą odpowiedzialne organy nadzorcze ustanowione na mocy RODO i EUDPR[21].

16. Zakres niniejszej opinii ogranicza się do aspektów wniosku związanych z przetwarzaniem danych osobowych, które to aspekty stanowią jeden z głównych filarów wniosku. Zważywszy że wniosek, jak wyjaśniono bardziej szczegółowo w opinii, budzi szereg obaw dotyczących ochrony podstawowych praw do prywatności i ochrony danych osobowych, opinia ta nie służy przedstawieniu wyczerpującego wykazu wszystkich problemów ani zaproponowaniu

[17] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie świadczenia usług związanych z cyfrowym euro przez dostawców usług płatniczych zarejestrowanych w państwach członkowskich, których walutą nie jest euro, oraz zmieniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1230, COM/2023/368 final.
[18] EBC, *Progress on the investigation phase of a digital euro – third report* (Postępy na etapie badania cyfrowego euro – trzecie sprawozdanie), 24 kwietnia 2023 r., dokument dostępny pod adresem: https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov230424_progress.en.pdf.
[19] Artykuł 133 TFUE.
[20] Zob. sekcja 11 niniejszej opinii.
[21] Motyw 12 wniosku.

alternatywnych przepisów lub innego brzmienia w każdym przypadku. Celem niniejszej opinii jest natomiast odniesienie się do głównych kluczowych aspektów wniosku dotyczących prywatności i ochrony danych.

3 UWAGI OGÓLNE

17. EROD i EIOD z zadowoleniem przyjmują zamiar zaprojektowania cyfrowego euro w sposób, który ogranicza przetwarzanie danych osobowych przez dostawców usług płatniczych, Eurosystem i dostawców usług wsparcia do tego, co jest niezbędne do zapewnienia właściwego funkcjonowania cyfrowego euro[22]. Jasno wynika to ze sposobu, w jaki we wniosku próbuje się ustanowić ramy dla danych osobowych, które mają być przetwarzane przez każdy z wyżej wymienionych podmiotów, określając kategorie danych osobowych wchodzących w zakres każdej czynności przetwarzania wymienionej w załącznikach towarzyszących wnioskowi. We wniosku podkreśla się również potrzebę odpowiedniej realizacji zasady uwzględniania ochrony danych już w fazie projektowania i uwzględniania domyślnej ochrony danych, gdyż wprowadza się wymóg wdrożenia najnowocześniejszych środków bezpieczeństwa i ochrony prywatności[23] oraz specjalnych zabezpieczeń w przypadkach wymagających szczególnej uwagi ze względu na związane z nimi ryzyko[24].

18. EROD i EIOD z zadowoleniem przyjmują również motyw 12 wniosku, który odnosi się do unijnych ram ochrony danych, a także motyw 70, w którym podkreśla się, że wysoki poziom prywatności i ochrony danych jest niezbędny, aby zapewnić zaufanie publiczne do cyfrowego euro, i odnosi się do wyżej wymienionego oświadczenia EROD wydanego w 2022 r. w sprawie wyborów projektowych dotyczących cyfrowego euro[25].

19. Biorąc pod uwagę fakt, że prywatność jest uważana za najważniejszą cechę cyfrowego euro zarówno dla osób prywatnych, jak i dla przedsiębiorstw[26], EROD i EIOD przypominają, że uwzględnienie ochrony danych już w fazie projektowania i domyślna ochrona danych powinny być wbudowane w projekt cyfrowego euro od samego początku, w tym w wybory techniczne, które zostaną dokonane przez EBC na podstawie art. 5 ust. 2 wniosku oraz w odniesieniu do dodatkowych aktów delegowanych i wykonawczych Komisji na podstawie art. 5 ust. 1 po przyjęciu wniosku. W tym względzie EROD i EIOD podkreślają znaczenie wdrażania technologii na rzecz ochrony prywatności (zwanych dalej „PET") podczas projektowania cyfrowego euro.

20. EROD i EIOD przypominają również, że zgodnie z orzecznictwem TSUE do wszelkich ograniczeń w korzystaniu z prawa do ochrony danych osobowych i poszanowania życia prywatnego

[22] Motywy 71 i 72 wniosku.
[23] Na przykład w art. 35 ust. 4 narzuca się wyraźną segregację danych osobowych w celu zapewnienia, aby Europejski Bank Centralny i krajowe banki centralne nie mogły bezpośrednio identyfikować poszczególnych użytkowników cyfrowego euro.
[24] Zob. ostatnie zdanie art. 35 ust. 8 wniosku.
[25] Oświadczenie EROD 04/2022 w sprawie wyborów projektowych dotyczących cyfrowego euro z perspektywy prywatności i ochrony danych, przyjęte 10 października 2022 r., dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf
[26] Strona 7 oceny skutków wniosku, SWD(2023) 233 final.

w odniesieniu do przetwarzania danych osobowych stosuje się test konieczności[27]. Obejmuje on ocenę, czy inne środki pozwoliłyby osiągnąć pożądany rezultat przy niższym stopniu ingerencji w określone prawo podstawowe. Ponadto, wprowadzając środki, które ingerują w podstawowe prawa do ochrony danych osobowych, prawodawca musi ocenić, czy znaczenie celu interesu ogólnego osiąganego przez przetwarzanie danych jest proporcjonalne do wagi ingerencji[28].

21. W tym kontekście EROD i EIOD uważają, że zadania związane z zarządzaniem użytkownikami (tj. zarządzanie rachunkami/portfelami cyfrowego euro, udostępnianie instrumentów płatniczych i zarządzanie nimi), zarządzaniem transakcjami (tj. inicjowanie transakcji, uwierzytelnianie i zatwierdzanie transakcji) oraz zarządzaniem płynnością (finansowanie i definansowanie) powinny być co do zasady jak najbardziej „zdecentralizowane". W związku z tym EROD i EIOD z zadowoleniem przyjmują fakt, że dystrybucja cyfrowego euro zgodnie z wnioskiem będzie prowadzona przez regulowanych pośredników finansowych w sposób zdecentralizowany, a nie bezpośrednio przez Eurosystem. W szczególności podejście zdecentralizowane mogłoby ułatwić osobom, których dane dotyczą, korzystanie ze swoich praw przed każdym pośrednikiem finansowym jako administratorem. W tym względzie sekcja 8 niniejszej wspólnej opinii zawiera kilka zaleceń i wzywa się w niej do wyjaśnienia ról i zadań, które – nie utrudniając funkcjonowania cyfrowego euro i roli EBC – mogłyby zostać przydzielone pośrednikom finansowym.

22. Ponadto, chociaż EROD i EIOD uznają potrzebę wprowadzenia limitów utrzymywanej kwoty cyfrowego euro dla każdego użytkownika cyfrowego euro, EROD i EIOD wskazują, że taka funkcja automatycznie oznacza utratę pełnej anonimowości i pewien stopień przetwarzania danych osobowych[29].

23. Jak już podkreślała EROD[30], wysoki poziom prywatności i ochrony danych jest niezbędny, aby zapewnić zaufanie obywateli do przyszłego cyfrowego euro i ostatecznie jego powodzenie. W związku z tym rejestrowanie wszystkich transakcji w cyfrowym euro w trybie online, niezależnie od ich kwoty, nie wydaje się zgodne z celem wniosku, jakim jest wspieranie ochrony danych jako kluczowej polityki prowadzonej przez Unię, ani ze znaczeniem, jakie obywatele przywiązują do prywatności w kontekście cyfrowego euro, co znalazło odzwierciedlenie w wyżej wspomnianym sondażu przeprowadzonym przez EBC w 2021 r[31]. W związku z tym EROD i EIOD uważają, że konieczne jest zapewnienie wysokiego poziomu prywatności nie tylko

[27] Wyrok z dnia 16 grudnia 2008 r., *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy*, C-73/07, EU:C:2008:727, pkt 56; wyrok z dnia 9 listopada 2010 r., sprawy połączone *Volker und Markus Schecke*, C-92/09 i C-93/09, EU:C:2010:662, pkt 77 i 86. Ponadto zob. EIOD, Wytyczne EIOD w sprawie oceny proporcjonalności środków ograniczających podstawowe prawa do prywatności i ochrony danych osobowych, 19 grudnia 2019 r., dokument dostępny pod adresem: https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

[28] Wyrok z dnia 1 sierpnia 2022 r., *OT i Vyriausioji tarnybinės etikos komisija*, C-184/20, EU:C:2022:601, pkt 98.

[29] Zob. w tym względzie sekcję 7 niniejszej opinii.

[30] Oświadczenie EROD 04/2022 w sprawie wyborów projektowych dotyczących cyfrowego euro z perspektywy prywatności i ochrony danych, przyjęte 10 października 2022 r., dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf

[31] EBC, *Report on the public consultation on a digital euro* (Sprawozdanie z konsultacji publicznych w sprawie cyfrowego euro), kwiecień 2021 r., dokument dostępny pod adresem: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html

w odniesieniu do płatności w cyfrowym euro w trybie offline, jak przewidziano obecnie we wniosku[32], lecz także w odniesieniu do transakcji płatniczych o niskiej wartości dokonywanych w cyfrowym euro w trybie online. EROD i EIOD zalecają osiągnięcie tego celu dzięki wprowadzeniu progu ochrony prywatności dla transakcji płatniczych w trybie online o niskiej wartości, jak szerzej opisano w sekcji 11 poniżej.

24. EROD i EIOD doceniają również wysiłki podjęte w celu zapewnienia, aby wniosek nie miał wpływu na stosowanie obowiązujących przepisów UE regulujących przetwarzanie danych osobowych, w tym na zadania i uprawnienia organów nadzorczych właściwych do monitorowania zgodności z przepisami o ochronie danych, jak wskazano w preambule wniosku[33]. Ważny aspekt dotyczy podstawy prawnej dla administratorów przetwarzających dane osobowe w kontekście wniosku oraz odpowiedniego przypisania ról i podziału odpowiedzialności między dostawcami usług płatniczych, Eurosystemem i dostawcami usług wsparcia. Ten element omówiono w sekcji 10 niniejszej wspólnej opinii.

25. Ponadto EROD i EIOD przyjmują do wiadomości, że art. 282 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej (zwanego dalej „TFUE") stanowi, że EBC jest niezależny w wykonywaniu swoich uprawnień oraz że instytucje, organy i jednostki organizacyjne UE, w tym Komisja i współprawodawcy, muszą szanować tę niezależność. W art. 130 TFUE dodaje się, że wykonując uprawnienia oraz zadania i obowiązki powierzone mu na mocy traktatów i statutu EBC, EBC nie zwraca się o instrukcje do instytucji, organów i jednostek organizacyjnych UE ani nie przyjmuje od nich instrukcji. Zgodnie z art. 132 TFUE EBC może uchwalać rozporządzenia i podejmować decyzje niezbędne do wykonania swoich zadań[34], co EBC robi często, również w odniesieniu do sposobu, w jakim przetwarza dane osobowe i nimi zarządza w kontekście swoich operacji[35]. Chociaż EROD i EIOD z należytym szacunkiem odnoszą się do autonomii decyzyjnej EBC, podkreślają również potrzebę ustanowienia we wniosku jasnych zasad, podlegających dyskusji legislacyjnej i zatwierdzeniu, dotyczących przetwarzania danych

[32] Artykuł 37 wniosku.

[33] Motyw 12 wniosku: „Wszelkie przetwarzanie danych osobowych na podstawie niniejszego rozporządzenia musi być zgodne z rozporządzeniem (UE) 2016/679 i rozporządzeniem (UE) 2018/1725 w ramach ich odpowiedniego zakresu stosowania. W związku z tym organy nadzorcze, o których mowa w rozporządzeniu (UE) 2016/679 i rozporządzeniu (UE) 2018/1725, są odpowiedzialne za nadzór nad przetwarzaniem danych osobowych prowadzonym w kontekście niniejszego rozporządzenia." Ponadto motyw 70 stanowi, że „Przetwarzanie danych osobowych w celu zapewnienia zgodności i w kontekście niniejszego rozporządzenia odbywałoby się zgodnie z rozporządzeniem (UE) 2016/679 i rozporządzeniem (UE) 2018/1725, a także, w stosownych przypadkach, zgodnie z dyrektywą 2002/58/WE."

[34] Znajduje to również odzwierciedlenie w art. 282 ust. 4 TFUE: „Europejski Bank Centralny przyjmuje środki niezbędne do wykonywania swoich zadań zgodnie z artykułami 127–133, artykułem 138 oraz warunkami przewidzianymi w Statucie ESBC i EBC."

[35] Zob. jako przykłady: Decyzja Europejskiego Banku Centralnego (UE) 2020/655 z dnia 5 maja 2020 r. przyjmująca zasady wykonawcze w zakresie ochrony danych w Europejskim Banku Centralnym i uchylająca decyzję EBC/2007/1 (EBC/2020/28) Dz.U. L 152 z 15.5.2020, s. 13-20; decyzja Europejskiego Banku Centralnego (UE) 2021/1486 z dnia 7 września 2021 r. przyjmująca zasady wewnętrzne dotyczące ograniczeń praw osób, których dane dotyczą, w związku z zadaniami Europejskiego Banku Centralnego w odniesieniu do nadzoru ostrożnościowego nad instytucjami kredytowymi (EBC/2021/42) Dz.U. L 328, 16.9.2021, s. 15-22; oraz motyw 10 decyzji Europejskiego Banku Centralnego (UE) 2022/1982 z dnia 10 października 2022 r. w sprawie korzystania z usług Europejskiego Systemu Banków Centralnych przez właściwe organy i przez organy współpracujące oraz zmieniającej decyzję EBC/2013/1 (EBC/2022/34) EBC/2022/34, Dz.U. L 272 z 20.10.2022, s. 29-35.

osobowych w kontekście emisji i korzystania z cyfrowego euro, z wyraźnymi zabezpieczeniami, tak aby zapewnić najwyższy możliwy poziom ochrony podstawowych praw i wolności.

26. W tym względzie EROD i EIOD rozumieją, że prawodawca Unii jest upoważniony do ustanowienia środków niezbędnych do używania euro jako jednej waluty, zgodnie z art. 133 TFUE, który stanowi podstawę prawną wniosku w Traktatach. Niemniej jednak instytucjonalne i prawne ograniczenia podstawy prawnej z art. 133 TFUE wynikające z zasad zapisanych w TFUE wymagają pozostawienia EBC pewnej swobody decyzyjnej w odniesieniu do szczegółowych środków, zasad i norm, które EBC poweźmie w celu wdrożenia środków przyjętych przez współprawodawców, takich jak te wymienione w art. 5 ust. 2 wniosku[36]. EROD i EIOD rozumieją również, że jest to powód, dla którego co do zasady we wniosku rzadko nakazuje się EBC wykonywanie pewnych zadań, ale często pozostawia się EBC swobodę uznania, czy je wykonać (poprzez użycie słowa „może" zamiast stwierdzenia, że EBC coś robi)[37]. W każdym razie, nawet w przypadkach, w których decyzje techniczne pozostają w gestii EBC, decyzje te podlegają potrzebie zapewnienia zgodności z unijnymi przepisami o ochronie danych, w tym z wymogami konieczności i proporcjonalności.

27. Wreszcie EROD i EIOD przyznają, że wniosek, oprócz podkreślenia potrzeby zapewnienia zgodności z RODO i EUDPR, przewiduje szczególne ograniczenia dla administratorów i zabezpieczenia dla osób, których dane dotyczą, w odniesieniu do przetwarzania danych osobowych. Odnosi się to na przykład do zakazu, o którym mowa w art. 37 ust. 2 wniosku, zabraniającego zatrzymywania danych dotyczących transakcji przez dostawców usług płatniczych lub przez Eurosystem w odniesieniu do transakcji płatniczych w cyfrowym euro dokonywanych w trybie offline. EROD i EIOD z zadowoleniem przyjmują również wymóg, zgodnie z którym EBC, na mocy art. 5 ust. 2 wniosku, musi skonsultować się z EIOD przed przyjęciem szczegółowych środków, zasad i norm, mogących mieć wpływ na ochronę danych.

4 ROZDZIAŁ I – PRZEDMIOT I DEFINICJE

28. EROD i EIOD zauważają, że art. 2 wniosku zawiera definicje niezbędne do zrozumienia wniosku jako całości. EROD i EIOD uważają jednak, że brakuje niektórych definicji lub niektóre definicje wymagają doprecyzowania w celu zapewnienia pewności prawa.

---

[36] Artykuł 5 ust. 2 stanowi, że „[w] ramach niniejszego rozporządzenia cyfrowe euro podlega również szczegółowym środkom, zasadom i normom, które mogą zostać przyjęte przez Europejski Bank Centralny zgodnie z jego kompetencjami. Jeżeli te szczegółowe środki, zasady i normy mają wpływ na ochronę praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych, Europejski Bank Centralny konsultuje się przed ich przyjęciem z Europejskim Inspektorem Ochrony Danych."

[37] Zob. przykład w motywie 25: „Europejski Bank Centralny **może** wspierać dostawców usług płatniczych w wykonywaniu zadania polegającego na egzekwowaniu wszelkich limitów utrzymywanej kwoty, w tym przez ustanowienie – samodzielnie lub wspólnie z krajowymi bankami centralnymi – pojedynczego punktu dostępu służącego do weryfikacji identyfikatorów użytkowników cyfrowego euro i powiązanych limitów utrzymywanej kwoty cyfrowego euro." Zob. również motyw 68: „Europejski Bank Centralny **może** ustanowić ogólny mechanizm wykrywania oszustw i zapobiegania im, który wspomoże działania w zakresie zwalczania oszustw prowadzone przez dostawców usług płatniczych w odniesieniu do transakcji płatniczych w cyfrowym euro dokonywanych w trybie online." (wyróżnienie dodane).

29. Po pierwsze centralnym elementem wniosku są dane generowane przez transakcje płatnicze. Mimo to we wniosku nie definiuje się tego, co obejmuje pojęcie „dane dotyczące transakcji" i czy sposób płatności w trybie offline lub online różni się pod względem rodzajów danych dotyczących transakcji, które to dane są generowane z transakcji lub oczekiwane i wymagane do pomyślnego wykonania transakcji. EROD i EIOD zalecają precyzyjne określenie rodzaju danych, które można by zaliczyć do kategorii „danych dotyczących transakcji". W tym względzie EROD i EIOD zauważają również, że w załącznikach III, IV i V do wniosku wykorzystuje się szerokie kategorie danych osobowych, które mają być przetwarzane przez różne podmioty. Te kategorie danych osobowych powinny być zdefiniowane w sposób bardziej precyzyjny, jak wyszczególniono w sekcji 9 niniejszej wspólnej opinii.

30. Ponadto EROD i EIOD zauważają, że we wniosku znajduje się klika odniesień do terminu „lokalne urządzenia pamięciowe". W szczególności we wniosku odniesienia do terminu „lokalne urządzenia pamięciowe" są w art. 2 pkt 15, art. 34 ust. 1 lit. c), art. 35 ust. 1 lit. c) i art. 37 ust. 4 lit. b), przy czym termin ten nie jest zdefiniowany w art. 2 wniosku. Zgodnie z motywem 34 wniosku: „Dostawcy usług płatniczych powinni rejestrować i wyrejestrowywać lokalne urządzenia pamięciowe na potrzeby transakcji płatniczych w cyfrowym euro dokonywanych przez klientów w trybie offline". W tym samym motywie określa się również, że dostawcy usług płatniczych będą tymczasowo przechowywać identyfikator lokalnego urządzenia służącego do przechowywania cyfrowego euro w trybie offline. W motywie 35 określa się dalej, że dostawcy usług płatniczych powinni rejestrować i wyrejestrowywać lokalne urządzenia do przechowywania transakcji płatniczych w cyfrowym euro dokonywanych przez klientów w trybie offline. Wreszcie motyw 75 stanowi, że w kontekście transakcji płatniczych w cyfrowym euro w trybie offline dostawcy usług płatniczych będą przetwarzać „[...] dane osobowe związane z deponowaniem lub wypłacaniem cyfrowych euro z rachunków płatniczych w cyfrowym euro w celu załadowania ich na lokalne urządzenia pamięciowe lub z lokalnych urządzeń pamięciowych na rachunki płatnicze w cyfrowym euro. *Obejmuje to identyfikator lokalnych urządzeń pamięciowych, który dostawcy usług płatniczych przypisują do użytkownika cyfrowego euro posiadającego cyfrowe euro w trybie offline.* Wydaje się zatem, że użycie we wniosku terminu „lokalne urządzenia pamięciowe" odnosi się do „urządzeń mobilnych". W art. 2 pkt 31 „urządzenia mobilne" są wyraźnie zdefiniowane jako „[...] urządzenie, które umożliwia użytkownikom cyfrowego euro autoryzację transakcji płatniczych w cyfrowym euro w trybie online lub offline, w tym w szczególności smartfony, tablety, inteligentne zegarki i wszelkiego rodzaju urządzenia nasobne". Ponadto EROD i EIOD zauważają, że w definicji „rachunku płatniczego w cyfrowym euro" w art. 2 pkt 5, używa się terminu „urządzenie służące do obsługi cyfrowego euro działające w trybie offline". W tym kontekście EROD i EIOD zalecają wyjaśnienie, czy „lokalne urządzenia pamięciowe" byłyby urządzeniami innymi niż „urządzenia mobilne" zdefiniowane w art. 2 pkt 31 wniosku, a jeżeli tak, to by w art. 2 wniosku zawrzeć odrębną definicję tego terminu. Wyjaśnienia takie powinny mieć zastosowanie odpowiednio do terminu „urządzenie służące do obsługi cyfrowego euro działające w trybie offline", o którym mowa w art. 2 pkt 5 wniosku.

31. Co więcej, EROD i EIOD zalecają doprecyzowanie definicji terminu „identyfikator użytkownika" w art. 2 pkt 27 wniosku. W art. 2 pkt 27 wniosku „identyfikator użytkownika" definiuje się jako „[...] unikatowy identyfikator utworzony przez dostawcę usług płatniczych prowadzącego dystrybucję cyfrowego euro, który jednoznacznie rozróżnia użytkowników cyfrowego euro do celów związanych z cyfrowym euro w trybie online, ale którego Europejski Bank Centralny i krajowe banki centralne nie mogą przypisać do możliwej do zidentyfikowania osoby fizycznej

lub prawnej". W tym względzie EROD i EIOD zauważają, że w załączniku III stwierdza się, iż „identyfikator użytkownika" zawierałby „nazwy posiadaczy lokalnych urządzeń pamięciowych". Innym przykładem jest związek między pojęciem „identyfikator użytkownika" zdefiniowanym w art. 2 pkt 27 wniosku i pojęciem „alias użytkownika" zdefiniowanym w art. 2 pkt 28 wniosku, z których oba wydają się wskazywać na metodę pseudonimizacji określoną w art. 4 pkt 5 RODO, chociaż jest to wyraźnie określone tylko w art. 2 pkt 28 wniosku.

32. Wreszcie EROD i EIOD zwracają uwagę, że w art. 22 ust. 3 wniosku używa się terminu „unikatowy numer rachunku płatniczego w cyfrowym euro", który jednak nie jest zdefiniowany w art. 2. W związku z tym, do celów pewności prawa, EROD i EIOD zalecają włączenie definicji „unikatowego numeru rachunku płatniczego w cyfrowym euro" do art. 2. Wprowadzenie takiej definicji pomogłoby również wyjaśnić różnicę między innymi typami identyfikatorów we wniosku, w szczególności „identyfikatorem użytkownika" zdefiniowanym w art. 2 pkt 27 i „aliasem użytkownika" zdefiniowanym w art. 2 pkt28 wniosku.

5 ROZDZIAŁ III – PRAWNY ŚRODEK PŁATNICZY

33. EROD i EIOD z zadowoleniem przyjmują cel polityki polegający na nadaniu cyfrowemu euro wartości prawnego środka płatniczego, tak jak ma to miejsce w przypadku monet i banknotów euro. Pieniądz elektroniczny musi uzupełniać, a nie zastępować, pieniądz fizyczny, który jest nadrzędnym środkiem płatniczym z punktu widzenia prywatności i swobód osobistych. W związku z tym EROD i EIOD z zadowoleniem przyjmują fakt, że obywatele zawsze będą mieli możliwość wyboru płatności w cyfrowym euro lub w gotówce, zgodnie z art. 12 ust. 2 wniosku.

6 ROZDZIAŁ IV – DYSTRYBUCJA

34. Wniosek reguluje dystrybucję cyfrowego euro za pośrednictwem istniejących ram prawnych UE w zakresie świadczenia usług płatniczych przewidzianych w dyrektywie (UE) 2015/2366 (PSD2)[38]. Dostawcy usług płatniczych mogą świadczyć usługi płatnicze związane z cyfrowym euro na rzecz szeregu kategorii osób fizycznych i prawnych zgodnie z art. 13 wniosku.

35. EROD i EIOD zauważają, że zgodnie z art. 13 ust. 1 lit. b) i c) wniosku cyfrowe euro można również dystrybuować do osób fizycznych lub prawnych, gdy ich miejsce zamieszkania lub siedziby nie znajduje się w państwach członkowskich, których walutą jest euro. Zgodnie z obecnym wnioskiem nie jest jednak jasne, w jakich przypadkach, w jaki sposób i dlaczego usługi płatnicze związane z cyfrowym euro mogą być ograniczone do wymienionych kategorii osób, których dane dotyczą, w jaki sposób wpływa to na przetwarzanie danych osobowych i czy dane osobowe są usuwane, gdy korzystanie z usług jest ograniczone. Nie jest również jasne, czy takie informacje należy określić w ramach niniejszego wniosku czy wniosku dotyczącego rozporządzenia w sprawie świadczenia usług związanych z cyfrowym euro przez dostawców usług płatniczych zarejestrowanych w państwach członkowskich, których walutą nie jest euro. W związku z tym EROD i EIOD zalecają doprecyzowanie kwestii przetwarzania prowadzonego

[38] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, Dz.U. L 337 z 23.12.2015, s. 35-37.

w ramach dystrybucji cyfrowego euro osobom fizycznym lub prawnym, gdy ich miejsce zamieszkania lub siedziby nie znajduje się w państwach członkowskich, których walutą jest euro, w niniejszym wniosku lub we wniosku dotyczącym rozporządzenia w sprawie świadczenia usług płatniczych związanych z cyfrowym euro przez dostawców usług płatniczych zarejestrowanych w państwach członkowskich, których walutą nie jest euro.

36. W art. 13 ust. 4 wniosku wymagana jest uprzednia zgoda użytkownika cyfrowego euro na powiązanie rachunku w cyfrowym euro z rachunkami płatniczymi w fiat, zarówno w celu finansowania, jak i definansowania rachunku w cyfrowym euro, oraz do uzupełniania płatności przekraczających limit utrzymywanej kwoty cyfrowego euro. Powiązanie to wiązałoby się z przetwarzaniem danych osobowych, ponieważ wymieniane byłyby informacje o wielu rachunkach płatniczych, które niekoniecznie są zapewniane przez tego samego dostawcę usług płatniczych. Z perspektywy ochrony danych EROD i EIOD uważają, że uprzedniej zgody nie należy interpretować jako zgody w rozumieniu RODO, ale raczej jako zabezpieczenie o charakterze umownym. W związku z tym EROD i EIOD zalecają zastąpienie wyrażenia „uprzednia zgoda" terminem „zezwolenie". Takie podejście byłoby zgodne z wnioskiem dotyczącym rozporządzenia w sprawie usług płatniczych[39] (zwanym dalej „PSR") i wnioskiem dotyczącym rozporządzenia w sprawie ram dostępu do danych finansowych (zwanym dalej „FIDA") [40] . W tym względzie EIOD sformułował już konkretne zalecenia w swoich wcześniejszych opiniach [41]. Zalecenia te, tj. zalecenia dotyczące konieczności rozróżnienia „zezwolenia" z jednej strony od podstawy prawnej zgody na przetwarzanie danych osobowych określonej w RODO, z drugiej strony, byłyby również ważne w świetle wniosku.

37. Ponadto EIOD i EROD pragną podkreślić, że wytyczne Urzędu ds. Przeciwdziałania Praniu Pieniędzy (zwanego dalej „AMLA") i Europejskiego Urzędu Nadzoru Bankowego (zwanego dalej „EUNB"), o których to wytycznych mowa w art. 14 ust. 5 wniosku, należy interpretować w ten sposób, że dostawcy usług płatniczych nie powinni rejestrować statusu potencjalnych użytkowników cyfrowego euro (np. jako osób ubiegających się o azyl lub beneficjentów ochrony międzynarodowej lub osób fizycznych bez stałego adresu lub obywateli państw trzecich, którym nie przyznano zezwolenia na pobyt), ponieważ mogłoby to stygmatyzować tych użytkowników.

[39] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego i zmieniającego rozporządzenie (UE) nr 1093/2010, COM/2023/367 final.
[40] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) nr 1095/2010 i (UE) 2022/2554, COM/2023/360 final.
[41] Opinia EIOD nr 38/2023 w sprawie wniosku dotyczącego rozporządzenia w sprawie ram dostępu do danych finansowych, przyjęta 22 sierpnia 2023 r., dokument dostępny pod adresem: https://edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf; Opinia EIOD nr 39/2023 w sprawie wniosku dotyczącego rozporządzenia w sprawie usług płatniczych w ramach rynku wewnętrznego oraz wniosku dotyczącego dyrektywy w sprawie usług płatniczych i usług związanych z pieniądzem elektronicznym w ramach rynku wewnętrznego, przyjęta 22 sierpnia 2023 r., dokument dostępny pod adresem: https://edps.europa.eu/system/files/2023-08/2023-0729_d2434_opinion_en.pdf

7 ROZDZIAŁ V – KORZYSTANIE Z CYFROWEGO EURO JAKO ŚRODKA PRZECHOWYWANIA WARTOŚCI I JAKO ŚRODKA PŁATNICZEGO

38. Co do zasady, art. 15 ust. 1 wniosku stanowi, że korzystanie z cyfrowego euro jako środka przechowywania wartości może podlegać ograniczeniom. Artykuł 16 ust. 1 wniosku stanowi, że EBC opracowuje instrumenty ograniczające korzystanie z cyfrowego euro jako środka przechowywania wartości oraz decyduje o ich parametrach i wykorzystaniu. Artykuł 35 ust. 8 wniosku stanowi, że do celów wspierania dostawców usług płatniczych w wykonywaniu obowiązku polegającego na egzekwowaniu limitów utrzymywanej kwoty zgodnie z art. 16 ust. 1 i zapewnieniu przenoszenia rachunków na wniosek użytkownika w trybie awaryjnym zgodnie z art. 31 ust. 2 EBC może – samodzielnie lub wspólnie z krajowymi bankami centralnymi – ustanowić pojedynczy punkt dostępu służący do weryfikacji identyfikatorów użytkowników cyfrowego euro i powiązanych limitów utrzymywanej kwoty cyfrowego euro. Artykuł 35 ust. 8 stanowi ponadto, że należy wdrożyć najnowocześniejsze środki bezpieczeństwa i ochrony prywatności w celu zapewnienia, aby niemożliwe było wywnioskowanie tożsamości poszczególnych użytkowników cyfrowego euro z informacji, do których podmioty inne niż dostawcy usług płatniczych, których klientem lub potencjalnym klientem jest dany użytkownik cyfrowego euro, uzyskały dostęp za pośrednictwem pojedynczego punktu dostępu. Co więcej, w motywie 77 wniosku stwierdzono, że pojedynczy punkt dostępu do identyfikatorów użytkowników cyfrowego euro i powiązanych limitów utrzymywanej kwoty cyfrowego euro jest niezbędny do zapewnienia sprawnego funkcjonowania cyfrowego euro w całej strefie euro, ponieważ użytkownicy cyfrowego euro mogą posiadać rachunki płatnicze w cyfrowym euro w różnych państwach członkowskich. Przy ustanawianiu pojedynczego punktu dostępu Eurosystem powinien zapewnić, aby przetwarzanie danych osobowych było zminimalizowane do tego, co jest bezwzględnie niezbędne, oraz aby w procesie tym uwzględniono ochronę danych w fazie projektowania i domyślną ochronę danych.

39. EROD i EIOD uznają, że w celu zapewnienia, aby nie doszło do przekroczenia limitu utrzymywanej kwoty przez użytkownika cyfrowego euro, który może posiadać różne konta cyfrowego euro u różnych dostawców usług płatniczych, nieunikniony jest pewien stopień przetwarzania danych osobowych. W tym względzie EROD i EIOD zauważają, że zgodnie z art. 35 ust. 8 wniosku „[...] EBC może – samodzielnie lub wspólnie z krajowymi bankami centralnymi – ustanowić pojedynczy punkt dostępu służący do weryfikacji identyfikatorów użytkowników cyfrowego euro i powiązanych limitów utrzymywanej kwoty cyfrowego euro, zgodnie z załącznikiem IV pkt 4 [...]". Ponadto motyw 77 odnosi się do faktu, że „[...] [p]rzy ustanawianiu pojedynczego punktu dostępu Europejski Bank Centralny i krajowe banki centralne powinny zapewnić, aby przetwarzanie danych osobowych było zminimalizowane do tego, co jest bezwzględnie niezbędne, oraz aby w procesie tym uwzględniono ochronę danych w fazie projektowania i domyślną ochronę danych".

40. Jednocześnie EROD i EIOD uważają, że wniosek nie wyjaśnia w wystarczającym stopniu konieczności i proporcjonalności przetwarzania danych osobowych wymienionych w pkt 4 załącznika IV. W związku z tym EROD i EIOD zalecają dalsze dopracowanie uzasadnienia konieczności i proporcjonalności pojedynczego punktu dostępu w motywie 77. Ponadto wniosek nie zawiera informacji na temat tego, w jaki sposób należy w tym zakresie wdrożyć domyślną ochronę danych i ochronę danych w fazie projektowania. EROD i EIOD zalecają

dokładniejsze określenie środków, które należy wdrożyć w celu uwzględnienia ochrony danych już w fazie projektowania i domyślnie od samego początku, w tym środków technicznych, które umożliwiłyby zdecentralizowane przechowywanie danych[42].

41. Ponadto we wniosku nie ma jasności co do tego, w jaki sposób dane osobowe wymienione w pkt 1 załącznika III musiałyby być przetwarzane przez dostawców usług płatniczych w celu egzekwowania limitów utrzymywanej kwoty w praktyce oraz jakie zabezpieczenia są zapewnione dla użytkowników cyfrowego euro (takie jak prawo do sprzeciwu wobec decyzji opartych na egzekwowaniu limitu utrzymywanej kwoty lub odwołania się od takich decyzji).

42. W art. 17 wniosku ogranicza się opłaty, które dostawcy usług płatniczych mogą pobierać od użytkowników za korzystanie z usług płatniczych związanych z cyfrowym euro. EROD i EIOD zauważają, że monitorując przestrzeganie przepisów przez dostawców usług płatniczych, EBC może przetwarzać dane osobowe, ponieważ EBC miałby prawo żądać od dostawców usług płatniczych przekazania „wszelkich informacji niezbędnych" do egzekwowania przepisów tegoż artykułu. W tym względzie EROD i EIOD uważają, że szerokie odniesienie do „wszelkich informacji niezbędnych" mogłoby mieć w praktyce nieproporcjonalne skutki dla gromadzenia danych osobowych. EROD i EIOD zalecają doprecyzowanie, że stosowanie tego przepisu powinno być zgodne z przepisami o ochronie danych zgodnie z celami przetwarzania, w tym z zasadą minimalizacji danych. Wnioski o udzielenie informacji składane przez EBC powinny zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinny dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych[43].

8 ROZDZIAŁ VII – CECHY TECHNICZNE

8.1 Formy obsługi cyfrowego euro w trybie offline i online

43. EROD i EIOD zauważają, że cyfrowe euro byłoby dostępne w dwóch formach: wersja w trybie online i wersja w trybie offline[44]. EROD i EIOD zdecydowanie popierają wprowadzenie trybu offline, ponieważ zapewniałby on wyższy poziom prywatności w porównaniu z trybem online. W szczególności EROD i EIOD z zadowoleniem przyjmują fakt, że zgodnie z art. 23 ust. 1 wniosku cyfrowe euro będzie dostępne dla transakcji płatniczych w cyfrowym euro dokonywanych zarówno w trybie offline, jak i w trybie online, począwszy od pierwszej emisji cyfrowego euro.

[42] Chociaż zrozumiałe jest, że informacje służące weryfikacji ogólnego limitu utrzymywanej kwoty użytkownika cyfrowego euro mogą pochodzić z więcej niż jednego rachunku w cyfrowym euro należącego do tego samego użytkownika, to w ramach wdrażania należy zbadać możliwość korzystania z PET, które pozwoliłyby uniknąć centralnego przechowywania danych osobowych wykorzystywanych do obliczeń i podejmowania stosownych decyzji (np. odrzucenie transakcji lub utworzenie nowego rachunku z określonym limitem utrzymywanej kwoty). W związku z tym bezpieczne obliczenia wielopodmiotowe można ocenić jako możliwą technikę (zob. Przewodnik ONZ dotyczący technologii na rzecz ochrony prywatności stosownych do statystyk urzędowych, sekcja 2.1 i powiązane przykłady, dokument dostępny pod adresem: https://unstats.un.org/bigdata/task-teams/privacy/guide/index.cshtml).

[43] Motyw 31 RODO

[44] Artykuł 23 ust. 1 wniosku.

44. W odniesieniu do trybu online EROD i EIOD zauważają, że – jak określono w art. 13 ust. 6 w związku z motywem 9 wniosku – umowy o prowadzenie takich rachunków i świadczenie takich usług byłyby podpisywane między użytkownikami a dostawcami usług płatniczych, tj. nie między użytkownikami a EBC. Takie podejście jest mile widziane, ponieważ odzwierciedla zdecentralizowane wdrażanie cyfrowego euro (mianowicie za pośrednictwem dostawców usług płatniczych), w przeciwieństwie do podejścia scentralizowanego, w pełni zarządzanego przez Eurosystem.

45. EROD i EIOD zauważają, że zgodnie z art. 22 ust. 3 wniosku „[k]ażdy rachunek płatniczy w cyfrowym euro ma unikatowy numer rachunku płatniczego w cyfrowym euro". Niemniej, jak już wskazano w sekcji 4 niniejszej opinii, termin „unikatowy numer rachunku płatniczego w cyfrowym euro" nie jest zdefiniowany w art. 2 wniosku. Brak takiej definicji budzi następujące wątpliwości: (i) kto będzie odpowiedzialny za zasady definiowania tego identyfikatora; (ii) w jaki sposób identyfikator byłby generowany: w sposób zdecentralizowany, na przykład z każdym dostawcą usług płatniczych definiującym swój własny format, lub w sposób bardziej scentralizowany, na przykład przez EBC; oraz (iii) co zawierałby ten identyfikator. W związku z tym EROD i EIOD zalecają sprecyzowanie powyższych elementów w nowej definicji „unikatowego numeru rachunku płatniczego w cyfrowym euro" zawartej w art. 2 oraz określenie wszelkich niezbędnych przepisów operacyjnych dotyczących jego wydania w art. 22.

8.2 Warunkowe transakcje płatnicze w cyfrowym euro

46. EROD i EIOD podkreślają, jak ważne jest zapewnienie, aby cyfrowe euro nie było „programowalnym pieniądzem". W tym względzie EROD i EIOD podkreślają rozróżnienie między programowalnym pieniądzem, zdefiniowanym we wniosku jako „jednostki pieniądza cyfrowego o logice wewnętrznej, która ogranicza pełną zamienność każdej jednostki" [45], a warunkowymi transakcjami płatniczymi w cyfrowym euro, rozumianymi jako transakcje płatnicze, które są zlecane automatycznie po spełnieniu wcześniej określonych warunków (np. okresowe płatności ratalne) uzgodnionych przez płatnika i odbiorcę[46].

47. Takie rozróżnienie przewidziano w art. 24 ust. 2 wniosku dotyczącym warunkowych transakcji płatniczych, w którym wyraźnie zakazuje się, aby cyfrowe euro było programowalnym pieniądzem. Ponadto motyw 55 stanowi, że „[w]ykorzystanie cyfrowego euro jako programowalnego pieniądza nie powinno stanowić celu ani skutku płatności warunkowych". Ponadto art. 12 ust. 1 stanowi, że cyfrowe euro musi być wymienialne na banknoty i monety euro według wartości nominalnej, co ponownie ilustruje nieprogramowalny charakter cyfrowego euro, ponieważ nie wiąże cyfrowego euro z określonymi zastosowaniami.

48. EROD i EIOD z zadowoleniem przyjmują te specyfikacje i zdecydowanie zalecają współprawodawcom, aby utrzymać te przepisy we wniosku. Rzeczywiście, z perspektywy prywatności i ochrony danych, programowalne cyfrowe euro wiązałoby się z niedopuszczalnie wysokim ryzykiem w zakresie ochrony danych. Mogłoby to na przykład umożliwić wyciąganie

[45] Artykuł 2 pkt 18 wniosku.
[46] Artykuł 2 pkt 17 wniosku.

wniosków o nawykach wydatkowych użytkownika cyfrowego euro już w chwili emisji cyfrowego euro lub doprowadzić do wprowadzenia dodatkowych mechanizmów w celu zapewnienia, aby użytkownicy nie obchodzili poleceń ograniczających korzystanie z cyfrowego euro.

8.3 Europejskie portfele tożsamości cyfrowej

49. Aby uzyskać dostęp do usług płatniczych związanych z cyfrowym euro i korzystać z nich, wniosek umożliwiłby użytkownikom cyfrowego euro korzystanie z usług typu front-end opracowanych przez dostawców usług płatniczych i EBC[47]. Takie usługi typu front-end definiuje się jako „wszystkie komponenty niezbędne do świadczenia usług na rzecz użytkowników cyfrowego euro, współdziałające za pośrednictwem zdefiniowanych interfejsów z rozwiązaniami typu back-end i innymi usługami typu front-end"[48]. Te usługi typu front-end *„[...] są interoperacyjne lub zintegrowane z europejskimi portfelami tożsamości cyfrowej",* a funkcje takich portfelów mogą być w szerszym zakresie wykorzystywane przez użytkowników cyfrowego euro, którzy o nie wystąpią[49].

50. EROD i EIOD przypominają, że planowane techniczne wdrożenie [50] wniosku dotyczącego rozporządzenia ustanawiającego europejskie portfele tożsamości cyfrowej, który jest obecnie przedmiotem negocjacji [51] , ostatecznie określi, czy należy zintegrować dodatkowe zabezpieczenia służące ochronie danych, czy już sam projekt będzie zgodny z przepisami o ochronie danych[52].

51. EROD i EIOD zauważają, że dostawcy usług płatniczych powinni przeprowadzać właściwą identyfikację użytkownika rachunku w cyfrowym euro za pomocą odpowiednich weryfikacji „znaj swojego klienta" na etapie onboardingu, do czego można wykorzystać europejskie portfele tożsamości cyfrowej. EROD i EIOD z zadowoleniem przyjmują fakt, że zgodnie z art. 25 ust. 2 wniosku korzystanie w tym celu z europejskich portfeli tożsamości cyfrowej odbywałoby się wyłącznie na wniosek użytkowników cyfrowego euro, a nie domyślnie, zgodnie z kluczową zasadą ochrony danych dotyczącą minimalizacji danych oraz obowiązkiem zapewnienia przez administratorów ochrony danych już w fazie projektowania i domyślnej ochrony danych[53].

[47] Artykuł 28 ust. 1 wniosku. W ust. 2 dodano, że EBC nie ma dostępu do żadnych danych osobowych w związku z usługami typu front-end opracowanymi przez EBC i wykorzystywanymi przez dostawców usług płatniczych.
[48] Artykuł 2 pkt 20 wniosku.
[49] Artykuł 25 ust. 1 i 2 wniosku.
[50] https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation.
[51] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3556.
[52] EIOD, Formalne uwagi na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia ram europejskiej tożsamości cyfrowej, 21 lipca 2021 r., s. 2, dokument dostępny pod adresem: https://edps.europa.eu/system/files/2021-07/21-07-28_formal_comments_2021-0598_d-1609_european_digital_identity_en.pdf
[53] Artykuł 5 ust. 1 lit. c) i art. 25 ust. 1 i 2 RODO.

8.4 Rozliczenie

52. EROD i EIOD zauważają, że ostateczne rozliczenie transakcji płatniczych w cyfrowym euro dokonywanych w trybie online odbywałoby się w przyjętej przez Eurosystem infrastrukturze rozrachunkowej służącej do obsługi cyfrowego euro [54]. Jest to odmienne podejście w porównaniu z rozliczaniem transakcji w ramach elektronicznych płatności prywatnych, które są realizowane pomiędzy instytucjami płatniczymi w sposób zdecentralizowany i w przypadku których Eurosystem nie ma dostępu do transakcji płatniczych. EROD i EIOD przyznają, że rozliczanie na poziomie makro transakcji w cyfrowym euro dokonywanych w trybie online musiałoby być przeprowadzane przez EBC, ponieważ cyfrowe euro, które nie zostało zdeponowane na poziomie banku, stanowi bezpośrednie zobowiązanie wobec EBC i krajowych banków centralnych[55], a zatem wymaga księgi na poziomie EBC.

53. Jednocześnie EROD i EIOD podkreślają, że infrastrukturze rozrachunkowej przyjętej przez EBC przechowywano by dane dotyczące wszystkich osób korzystających z cyfrowego euro w trybie online w sposób scentralizowany i zawierałaby ona informacje szczególnie chronione, takie jak dane uwierzytelniające użytkownika [56]. Ze względu na skalę i charakter danych przechowywanych w sposób scentralizowany konsekwencje wszelkich naruszeń bezpieczeństwa danych mogłyby potencjalnie zaszkodzić bardzo dużej liczbie osób fizycznych. EROD i EIOD są gotowe pomóc w ocenie odpowiednich zabezpieczeń, które mają zostać wdrożone w tym zakresie.

54. W tym kontekście EROD i EIOD z zadowoleniem przyjmują motyw 71 wniosku, który stanowi, że „Rozliczanie transakcji w cyfrowym euro powinno odbywać się w taki sposób, aby ani Europejski Bank Centralny, ani krajowe banki centralne nie mogły przypisać danych do zidentyfikowanego lub możliwego do zidentyfikowania użytkownika cyfrowego euro". EROD i EIOD z zadowoleniem przyjmują również motyw 76, który stanowi, że „Europejski Bank Centralny i krajowe banki centralne mogą przetwarzać dane osobowe w zakresie, w jakim jest to konieczne do realizacji zadań, które są niezbędne do prawidłowego funkcjonowania cyfrowego euro". Jednocześnie EROD i EIOD wskazują, że wniosek nie ustanawia wiążącego obowiązku, który zapewniałby pseudonimizację danych dotyczących transakcji względem EBC i krajowych banków centralnych. EROD i EIOD zalecają zatem wprowadzenie wyraźnego obowiązku pseudonimizacji danych dotyczących transakcji względem EBC i krajowych banków centralnych w części normatywnej wniosku, zamiast odnosić się do niego jedynie w motywie 76 wniosku.

8.5 Ogólny mechanizm wykrywania oszustw i zapobiegania im

55. EROD i EIOD zauważają, że art. 32 ust. 1 wniosku odnosi się do mechanizmu wykrywania oszustw i zapobiegania im (zwanego dalej „FDPM"), który EBC może zdecydować się ustanowić w celu ułatwienia realizacji zadań związanych z wykrywaniem oszustw i zapobieganiem im,

[54] Artykuł 30 ust. 2 i motyw 64 wniosku.
[55] Motyw 9 wniosku.
[56] Punkt 2 załącznika IV do wniosku.

które to zadania dostawcy usług płatniczych muszą wykonywać na mocy dyrektywy 2015/2366 „[...] aby zapewnić sprawne i skuteczne funkcjonowanie cyfrowego euro". FDPM może być obsługiwany bezpośrednio przez EBC lub przez dostawców usług wsparcia wyznaczonych przez EBC. EROD i EIOD z zadowoleniem odnotowują, że w art. 32 ust. 2 nakłada się na EBC obowiązek konsultowania się z EIOD przed opracowaniem szczegółowych specyfikacji elementów operacyjnych FDPM.

56. Zgodnie z art. 32 ust. 3 FDPM miałby: „ocenić w czasie rzeczywistym ekspozycję na ryzyko wystąpienia oszustwa przy transakcjach w cyfrowym euro dokonywanych w trybie online, na wyłączny użytek dostawców usług płatniczych, przed wprowadzeniem transakcji do infrastruktury rozrachunkowej służącej do obsługi cyfrowego euro"[57] oraz stanowić „wsparcie dla dostawców usług płatniczych w wykrywaniu oszukańczych transakcji wśród rozliczonych już transakcji płatniczych w cyfrowym euro dokonywanych w trybie online"[58].

57. W tym względzie należy zauważyć, że dostawcy usług płatniczych prowadzą już działania w zakresie wykrywania oszustw, w szczególności w ramach swoich zobowiązań prawnych wynikających z drugiej dyrektywy w sprawie usług płatniczych[59]. Co więcej, art. 32 ust. 1 stanowi, że dostawcy usług płatniczych prowadziliby takie działania również w zakresie wykrywania oszustw w kontekście cyfrowego euro. Jednocześnie w motywie 68 wyjaśnia się, że planowana FDPM jest konieczna, ponieważ *„ [s]kuteczność [szybkiego] wykrywania oszustw można [...] zwiększyć dzięki informacjom o potencjalnie oszukańczych działaniach, pochodzącym od innych dostawców usług płatniczych".* W tym samym motywie dodaje się ponadto, że: *„Taka ogólna funkcja wykrywania oszustw występuje w porównywalnych systemach płatności i jest niezbędna do osiągnięcia wyraźnie niskiej liczby oszustw, a tym samym do zagwarantowania bezpieczeństwa cyfrowego euro zarówno konsumentom, jak i akceptantom".*

58. EROD i EIOD przyznają, że ustanowienie FDPM mogłoby sprawić, że szybkie wykrywanie oszustw będzie bardziej skuteczne. Niemniej jednak EROD i EIOD uważają, że zwiększenie skuteczności szybkiego wykrywania oszustw nie jest samo w sobie wystarczające, aby w świetle Karty ingerencja w podstawowe prawa do prywatności i ochrony danych, którą pociągałby za sobą planowany system, była konieczna. Ponadto EROD i EIOD uważają, że wniosek nie przewiduje jasnych i precyzyjnych zasad regulujących zakres i stosowanie planowanego FDPM, w tym w odniesieniu do charakteru wsparcia, które EBC ma zapewnić dostawcom usług płatniczych. Dla przykładu, motyw 68 wydaje się sugerować, że FDPM pełniłby rolę porównywalną do ogólnej funkcji istniejącej w innych schematach płatniczych. W art. 32 wniosku nie ma jednak rozróżnienia między z jednej strony rolą i zadaniami EBC jako organu odpowiedzialnego za monitorowanie ogólnego systemu nadzorowania wykonywania

[57] COM (2023) 369 final, art. 32 ust. 3 lit. a).
[58] COM (2023) 369 final, art. 32 ust. 3 lit. b).
[59] Zob. art. 72 ust. 2 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG).
Dz.U. L 337 z 23.12.2015, s. 35-127.

działań w zakresie zwalczania oszustw, a z drugiej strony rolą i zadaniami dostawców usług płatniczych. W związku z tym EROD i EIOD są zdania, że art. 32 wniosku nie jest przewidywalny, stąd podważa pewność prawa i zdolność do oceny konieczności ustanowienia takiego środka, co jest niezbędnym wymogiem dla każdego ograniczenia podstawowego prawa do ochrony danych na mocy art. 52 ust. 1 Karty.

59. Co więcej, chociaż EROD i EIOD uznają, że ogólne funkcje wykrywania oszustw istnieją w komercyjnych schematach płatności, jak podkreślono w motywie 68, to EROD i EIOD przypominają, że działania te opierają się na wykorzystaniu różnych technologii, od tradycyjnych rozwiązań polegających na wykrywaniu oszustw na podstawie reguł po systemy oparte na analizie w czasie rzeczywistym, uczeniu maszynowym, a także sztucznej inteligencji, z których wszystkie wymagają przetwarzania dużych ilości danych osobowych[60]. W związku z tym zapewnienie ochrony praw podstawowych w tym kontekście wymaga starannego rozważenia konieczności i proporcjonalności przetwarzania danych osobowych, jak również solidnych zabezpieczeń. Ta ocena jest jeszcze ważniejsza, gdy weźmie się pod uwagę taki system jak planowany FDPM.

60. Podsumowując, EROD i EIOD uważają, że we wniosku nie wykazano w wystarczającym stopniu konieczności ustanowienia przez EBC ogólnego mechanizmu FDPM prowadzonego przez EBC oraz wprowadzenia odpowiednich zabezpieczeń niezbędnych do zapewnienia zgodności przetwarzania z zasadą proporcjonalności. EROD i EIOD wzywają zatem współprawodawców do dalszego wykazania takiej konieczności lub, jeżeli takiej konieczności nie można wykazać, uwzględnienia mniej inwazyjnych środków z punktu widzenia ochrony danych. W przypadku wykazania konieczności zastosowania takiego mechanizmu należy określić szczegółowe zabezpieczenia, w tym w odniesieniu do odpowiedniego ograniczenia przechowywania, w celu zapewnienia, aby mechanizmy zwalczania oszustw nie spowodowały nadmiernej i nieproporcjonalnej ingerencji w podstawowe prawa i wolności do prywatności i ochrony danych osobowych osób fizycznych[61].

61. Wreszcie EROD i EIOD zauważają, że planowany FDPM podlegałaby licznym ograniczeniom i zabezpieczeniom, w tym temu, że dostawcy usług płatniczych byliby zobowiązani do wdrażania odpowiednich środków technicznych i organizacyjnych „w celu zapewnienia, aby w ramach usług wsparcia nie można było bezpośrednio zidentyfikować użytkowników cyfrowego euro na podstawie informacji przekazanych na potrzeby mechanizmu wykrywania oszustw i zapobiegania im”[62]. Podobnie w przypadku gdy EBC postanowi nie powierzać dostawcom usług wparcia zadań związanych z FDPM, EBC i krajowe banki centralne nie

[60] Na przykład międzynarodowe prywatne systemy kart płatniczych obsługują ogólne mechanizmy wykrywania oszustw przetwarzające szeroki zakres danych osobowych, w tym biometryczne dane behawioralne, które są wykorzystywane do analizy wzorców zachowań konsumentów w celu wykrywania oszustw.

[61] w szczególności szybki rozwój technologii, takich jak poufne przetwarzanie danych i szyfrowanie homomorficzne, może pozwolić na wdrożenie dynamicznych identyfikatorów, które nie pociągają za sobą ani identyfikacji poszczególnych użytkowników cyfrowego euro, ani ich indywidualnego profilowania na poziomie FDPM.

[62] Artykuł 32 ust. 4 wniosku.

powinny bezpośrednio identyfikować indywidualnych użytkowników cyfrowego euro [63]. Jednocześnie w motywie 68 wyjaśniono, że przekazywanie informacji między dostawcami usług płatniczych a FDPM powinno być objęte najnowocześniejszymi środkami bezpieczeństwa i ochrony prywatności, które zapewnią, aby poszczególni użytkownicy cyfrowego euro nie mogli zostać zidentyfikowani przez FDPM.

62. Niezależnie od potrzeby dalszego uzasadnienia konieczności i proporcjonalności FDPM, jak wskazano powyżej, EROD i EIOD uważają również, że ani dostawcy usług wsparcia, ani EBC lub krajowe banki centralne nie powinny być w stanie zidentyfikować użytkowników cyfrowego euro na podstawie informacji przekazanych do FDPM, zgodnie z definicją pseudonimizacji zawartą w art. 4 pkt 5 RODO. W związku z tym art. 32 ust. 4 i art. 35 ust. 7 wniosku należy zmienić zgodnie z definicją pseudonimizacji zawartą w art. 4 pkt 5 RODO, tj. przez wprowadzenie zapisu, że dostawcy usług płatniczych z jednej strony oraz EBC i krajowe banki centralne z drugiej strony powinni wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia, aby przetwarzanie danych osobowych odbywało się w taki sposób, by nie można ich było już przypisać indywidualnemu użytkownikowi cyfrowego euro bez użycia dodatkowych informacji. Ponadto EROD i EIOD zalecają przyjęcie najbardziej odpowiednich PET, które zapewniłyby najwyższy poziom ochrony z punktu widzenia ochrony danych przy jednoczesnym uwzględnieniu właściwych potrzeb w zakresie użyteczności i skalowalności.

9 BEZPIECZEŃSTWO CYBERNETYCZNE I ODPORNOŚĆ OPERACYJNA

63. EROD i EIOD dostrzegają potencjalne zagrożenia, na jakie mogą być narażone płatności w cyfrowym euro z punktu widzenia IT i cyberbezpieczeństwa. W tym względzie EROD i EIOD przypominają, jak podkreślono w ocenie skutków towarzyszącej wnioskowi[64], że akt w sprawie operacyjnej odporności cyfrowej [65] miałby zastosowanie do dostawców usług płatniczych i dostawców usług wsparcia oraz że zgodnie z oczekiwaniami Eurosystem ma podlegać nowemu rozporządzeniu w sprawie cyberbezpieczeństwa[66], które jest obecnie przedmiotem negocjacji.

64. W związku z tym EROD i EIOD zalecają umieszczenie w motywie odniesienia do mających zastosowanie ram prawnych w zakresie cyberbezpieczeństwa.

65. Ponadto w przypadku braku nadrzędnego prawa w zakresie cyberbezpieczeństwa, które miałoby zastosowanie do wszystkich właściwych podmiotów, EROD i EIOD przypominają, że ważne jest zapewnienie spójnego podejścia między bezpieczeństwem i odpornością

[63] Artykuł 35 ust. 7 wniosku.
[64] SWD(2023) 233 final, s. 87.
[65] 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, PE/41/2022/INIT, Dz.U. L 333 z 27.12.2022, s. 1-79.
[66] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii, COM(2022) 122 final.

operacyjną: z jednej strony infrastruktury cyfrowego euro, a z drugiej – infrastruktury dostawców usług płatniczych. Ponadto wszelkie przepisy dotyczące cyberbezpieczeństwa i odporności operacyjnej wysokiego poziomu, które są specyficzne dla infrastruktury cyfrowego euro i które nie byłyby objęte wyżej wymienionymi ramami cyberbezpieczeństwa (takie jak wszelkie ewentualne odniesienia do certyfikacji), powinny zostać włączone do części normatywnej omawianego wniosku.

10 ROZDZIAŁ VIII – PRYWATNOŚĆ I OCHRONA DANYCH

66. EROD i EIOD z zadowoleniem przyjmują cel wyrażony w motywie 70 wniosku, w którym przypomina się o potrzebie ustanowienia wysokiego poziomu prywatności i ochrony danych, aby zapewnić zaufanie Europejczyków do przyszłego cyfrowego euro oraz realizacji innych praw i wolności zapisanych w Karcie. W związku z tym EROD i EIOD przypominają, że aby osiągnąć ten cel, przepisy powinny konkretnie i wyraźnie odnosić się do aspektów cyfrowego euro związanych z ochroną danych osobowych[67].

67. W tym kontekście EROD i EIOD z zadowoleniem przyjmują ustanowienie w rozdziale VIII celów, dla których można przetwarzać dane osobowe w celu zapewnienia cyfrowego euro. Rozdział ten służy również określeniu odpowiednich obowiązków dostawców usług płatniczych, EBC lub krajowych banków centralnych oraz, w stosownych przypadkach, dostawców usług wsparcia w odniesieniu do operacji przetwarzania. Niemniej, jak wskazano poniżej[68], EROD i EIOD uważają, że współprawodawcy powinni bardziej doprecyzować te aspekty, jak również podstawy prawne mające zastosowanie do tych operacji przetwarzania.

68. Ponadto EROD i EIOD z zadowoleniem przyjmują podejście przyjęte we wniosku, zakładające uregulowanie (w załącznikach do wniosku) kategorii danych osobowych, które mogą być przetwarzane przez każdy z podmiotów uczestniczących w emisji cyfrowego euro. Jednocześnie EROD i EIOD zauważają, że załączniki te nie zawsze zawierają wyczerpujący wykaz rodzajów danych osobowych, które mają być przetwarzane, co podważa pewność prawa. EROD i EIOD zachęcają współprawodawców do dalszego doprecyzowania tych wykazów – w miarę możliwości z uwzględnieniem potrzeb odpowiednich zainteresowanych stron oraz poszanowania zasady minimalizacji danych i obowiązku uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych.

10.1 Artykuł 34: Przetwarzanie przez dostawców usług płatniczych

69. EROD i EIOD uznają, że art. 34 ust. 1 wniosku ma na celu określenie celów, dla których dostawcy usług płatniczych będą przetwarzać dane osobowe podczas świadczenia usług związanych z cyfrowym euro. Użycie wyrażenia „w tym” w art. 34 ust. 1 lit. a) i c) wniosku budzi jednak niepewność prawną co do dokładnych celów, dla których dostawcy usług płatniczych mogą przetwarzać dane osobowe. EROD i EIOD uważają, że cele nie powinny być wyrażane

[67] Oświadczenie EROD 04/2022 w sprawie wyborów projektowych dotyczących cyfrowego euro z perspektywy prywatności i ochrony danych, przyjęte 10 października 2022 r., dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf
[68] Zob. pkt 74–76, 81, 85 i 86 poniżej.

w sposób ogólny, lecz raczej jasny i precyzyjny, i powinny być obiektywnie powiązane z zadaniami powierzonymi tym dostawcom na mocy wniosku. W związku z tym EROD i EIOD zalecają, aby art. 34 ust. 1 lit. a) i c) w sposób wyczerpujący odnosił się do odpowiednich zadań powierzonych dostawcom usług płatniczych, w odniesieniu do których to zadań dane osobowe mogą być przetwarzane na podstawie wniosku.

Podstawy prawne mające zastosowanie do przetwarzania prowadzonego przez dostawców usług płatniczych

70. EROD i EIOD uważają, że wniosek nie jest wystarczająco jasny, jeśli chodzi o podstawę prawną, na jakiej dostawcy usług płatniczych będą opierać przetwarzanie danych do celów, o których mowa w art. 34 ust. 1 wniosku, ponieważ zawiera on odniesienia do opierania się zarówno na interesie publicznym, jak i na obowiązku prawnym. W szczególności wniosek stanowi, że dostawcy usług płatniczych wykonują zadania wymienione w art. 34 ust. 1 wniosku „w interesie publicznym", co oznacza, że wykonują zadanie w interesie publicznym zgodnie z art. 6 ust. 1 lit. e) RODO, przetwarzając dane osobowe użytkowników do celów wymienionych w art. 34 wniosku. Ponadto EROD i EIOD zauważają, że chociaż motyw 73 wniosku wyraźnie odnosi się do art. 6 ust. 1 lit. c) RODO i uznaje się w nim, że przetwarzanie prowadzone przez dostawców usług płatniczych jest „niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze zgodnie z niniejszym rozporządzeniem", to stwierdza się w nim również, że przetwarzanie danych osobowych do celów zadań, o których mowa w art. 34 ust. 1 lit. a)–c), jest zadaniem leżącym „w interesie publicznym i [ma] zasadnicze znaczenie dla ochrony obywateli korzystających z cyfrowego euro, a także dla stabilności i integralności unijnego systemu finansowego". Jednocześnie w motywie 73 wniosku wskazuje się, że dostawcy usług płatniczych mogą również przetwarzać dane osobowe w celu wypełnienia dotychczasowych zadań leżących w interesie publicznym lub w celu wypełnienia zobowiązania prawnego ustanowionego w prawie Unii.

71. W tym względzie EROD i EIOD pragną przypomnieć, że zgodnie z RODO przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy zastosowanie ma odpowiednia podstawa prawna określona w art. 6 ust. 1 RODO, przy czym zastosowanie jednej z tych sześciu podstaw musi zostać ustalone przed rozpoczęciem czynności przetwarzania i w odniesieniu do określonego celu[69]. W szczególności, chociaż EROD i EIOD rozumieją pogląd Komisji, że cyfrowe euro jest publicznym towarem wspólnego dobra, EROD i EIOD są zdania, że w zakresie, w jakim cele wymienione w art. 34 ust. 1 lit. a)–c) wniosku wynikają z obowiązków prawnych, którym podlegają dostawcy usług płatniczych na mocy niniejszego wniosku[70], art. 6

[69] Wytyczne EROD 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, przyjęte 4 maja 2020 r., pkt 121, dokument dostępny pod adresem: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (również odniesienie w przypisie 59 do faktu, że zgodnie z art. 13 ust. 1 lit. c) i art. 14 ust. 1 lit. c) RODO administratorzy są zobowiązani do informowania osób, których dane dotyczą, o podstawie prawnej, na której opierają się w odniesieniu do każdego przetwarzania).

[70] Zob. na przykład użycie formy stwierdzającej w art. 13 ust. 2 („[d]ostawcy usług płatniczych [...] **umożliwiają** użytkownikom cyfrowego euro ręczne lub automatyczne finansowanie lub definansowanie rachunków płatniczych w cyfrowym euro"), ust. 3 („[d]ostawcy usług płatniczych **udostępniają** użytkownikom cyfrowego euro funkcje finansowania i definansowania), ust. 4 („[d]ostawcy usług płatniczych [...] **umożliwiają** użytkownikom cyfrowego euro [...]"), art. 16 ust. 1 („[d]ostawcy usług płatniczych [...] stosują te ograniczenia do

ust. 1 lit. c) RODO wydaje się najodpowiedniejszą podstawą tych czynności przetwarzania. W związku z tym EROD i EIOD zalecają, aby współprawodawcy wyjaśnili w motywie 73 i art. 34 wniosku, że przetwarzanie, które ma być prowadzone zgodnie z art. 34 ust. 1 lit. a)–c) wniosku, odbywa się na podstawie obowiązku prawnego (art. 6 ust. 1 lit. c) RODO).

72. Ponadto EROD i EIOD zalecają wyjaśnienie w motywie 73 i art. 34 wniosku, że czynności przetwarzania wykonywane zgodnie z art. 34 ust. 1 lit. d) i e) wniosku są prowadzone na podstawie obowiązku prawnego (art. 6 ust. 1 lit. c) RODO), ponieważ jest to najbardziej odpowiednia podstawa prawna, biorąc pod uwagę, że przetwarzanie do tych celów jest wymagane przez prawo Unii.

73. Co więcej, EROD i EIOD pragną wyjaśnić, że podstawa prawna określona w art. 34 nie powinna mieć zastosowania do usług płatniczych związanych z cyfrowym euro rozwijanych i świadczonych przez dostawców usług płatniczych w uzupełnieniu podstawowych usług płatniczych związanych z cyfrowym euro[71], do których miałby zastosowanie art. 6 ust. 1 lit. b) RODO lub art. 6 ust. 1 lit. a) RODO, biorąc pod uwagę, że usługi te podlegają dyrektywie 2015/2366[72].

Rodzaje danych osobowych przetwarzanych przez dostawców usług płatniczych

74. W art. 34 ust. 2 wniosku wyjaśnia się, że kategorie danych osobowych, które powinny być przetwarzane w celach wymienionych w art. 34 ust. 1 lit. a)–c), są określone w załączniku III do wniosku. EROD i EIOD uważają, że wskazane byłoby dalsze doprecyzowanie w załączniku III dokładnego rodzaju danych, które mogą być przetwarzane przez dostawców usług płatniczych. Jasne określenie rodzajów danych osobowych jest tym bardziej istotne, że dla ważności podstawy prawnej, o której mowa w art. 6 ust. 1 lit. c) RODO, sam obowiązek prawny musi być precyzyjny, musi mieć wystarczająco jasne umocowanie w prawie w odniesieniu do przetwarzania danych osobowych, którego wymaga, a administrator nie może mieć nadmiernej swobody uznania co do sposobu wypełnienia tego obowiązku prawnego[73].

75. W szczególności EROD i EIOD zalecają współprawodawcom dalsze określenie rodzajów danych osobowych, które można zakwalifikować do następujących kategorii danych:
    - „identyfikator użytkownika" *w* pkt 1 ppkt (i) załącznika III, w odniesieniu do którego w pkt 3 ppkt (i) załącznika III wskazuje się, że może on obejmować, między innymi, „nazwy

rachunków płatniczych w cyfrowym euro") wniosku, jak również w art. 23 ust. 1 („[c]yfrowe euro **jest dostępne** na potrzeby transakcji płatniczych w cyfrowym euro dokonywanych zarówno w trybie offline, jak i w trybie online"), art. 30 ust. 3 wniosku („[o]stateczne rozliczenie transakcji płatniczych w cyfrowym euro dokonywanych w trybie offline **odbywa się** w chwili zaktualizowania rejestrów dotyczących odnośnych zasobów cyfrowego euro w lokalnych urządzeniach pamięciowych płatnika i odbiorcy") (uwypuklenie dodane).

[71] W tym względzie EROD i EIOD zauważają, że zgodnie z motywem 30 dokładny charakter tych usług zostanie opracowany przez dostawców usług płatniczych, a zatem nie jest zdefiniowany we wniosku.

[72] W odniesieniu do stosowania art. 6 ust. 1 lit. b) i art. 6 ust. 1 lit. a) RODO odsyłamy do Wytycznych EROD 06/2020 w sprawie wzajemnych zależności miedzy dyrektywą PSD2 i RODO, przyjętych 15 grudnia 2020 r., dokument dostępny pod adresem:https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpubliccons ultation_en.pdf

[73] Zob. art. 6 ust. 1 lit. c), art. 6 ust. 3 lit. a) i motyw 41 RODO.

posiadaczy lokalnych urządzeń pamięciowych”[74]. Ponadto EROD i EIOD zauważają, że termin „identyfikator użytkownika” jest również używany w pkt 3 ppkt (i) załącznika III, przy czym punkt ten ma zastosowanie do przetwarzania w celu dostarczania cyfrowego euro w trybie offline (art. 34 ust. 1 lit. c)). Jednocześnie zgodnie z art. 2 pkt 27 „»identyfikator użytkownika« oznacza unikatowy identyfikator utworzony przez dostawcę usług płatniczych [...] do celów związanych z cyfrowym euro w trybie online [...]”, co wydaje się być sprzeczne z użyciem tego terminu w pkt 3 ppkt (i) załącznika III.

- *„informacje dotyczące rachunków płatniczych w cyfrowym euro”* w pkt 1 ppkt (iii) załącznika III. Chociaż EROD i EIOD zauważają, że mogą one obejmować „informacje dotyczące zasobów cyfrowego euro użytkownika cyfrowego euro i unikatowy numer rachunku płatniczego w cyfrowym euro”, to pkt 1 ppkt (iii) załącznika III nie zapewnia wystarczającej jasności co do tego, jakie inne rodzaje danych osobowych należałyby do tej kategorii;
- „informacje dotyczące transakcji płatniczych w cyfrowym euro dokonywanych w trybie online” w pkt 1 ppkt (iv) załącznika III. Chociaż EROD i EIOD zauważają, że mogą one obejmować „identyfikator transakcji i kwot[ę] transakcji”, to pkt 1 ppkt (iv) załącznika III nie zapewnia wystarczającej jasności co do tego, jakie inne rodzaje danych osobowych zaliczałyby się do tej kategorii;
- „Unikatowy numer rachunku płatniczego w cyfrowym euro” w pkt 2 ppkt (iii) załącznika III. Biorąc pod uwagę, że w art. 2 wniosku nie przedstawiono żadnej definicji[75], nie jest jasne, co zostałoby zawarte w tym identyfikatorze ani w jaki sposób i przez kogo zostałby on wygenerowany (tj. czy w sposób zdecentralizowany, w którym każdy dostawca usług płatniczych określa swój własny format, czy też w bardziej scentralizowany sposób przez EBC).

76. Wreszcie EROD i EIOD zauważają brak wykazu kategorii i rodzajów danych osobowych do celów wymienionych w art. 34 ust. 1 lit. d) i e) i zalecają, aby współprawodawcy szczegółowo opracowali i zamieścili w załączniku III wykazy kategorii i konkretnych rodzajów danych osobowych, które mają być przetwarzane do tych celów .

Podział odpowiedzialności między dostawcami usług płatniczych

77. Zgodnie z art. 34 ust. 3 wniosku za administratorów danych osobowych w odniesieniu do celów, o których mowa w art. 34 ust. 1, należy uznać dostawców usług płatniczych. We wniosku określa się również, że gdy rachunek płatniczy w cyfrowym euro prowadzony przez jednego dostawcę usług płatniczych jest powiązany z rachunkiem płatniczym w niecyfrowym euro prowadzonym przez innego dostawcę usług płatniczych zgodnie z art. 13 ust. 4 wniosku, wówczas ci dostawcy usług płatniczych muszą być współadministratorami. EROD i EIOD pragną przypomnieć, że zgodnie z art. 26 ust. 1 RODO w przypadku braku odpowiednich obowiązków określonych w kontekście omawianego wniosku do współadministratorów należeć będzie określenie odpowiednich zakresów ich odpowiedzialności w odniesieniu do takiego przetwarzania, w szczególności w odniesieniu do wykonywania przez osobę, której dane

[74] Zob. sekcja 4 niniejszej opinii.
[75] Zob. sekcja 4 niniejszej opinii.

dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO[76].

Obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych przez dostawców usług płatniczych

78. EROD i EIOD z zadowoleniem przyjmują wprowadzenie w art. 34 ust. 4 projektu obowiązku wdrożenia przez dostawców usług płatniczych odpowiednich środków technicznych i organizacyjnych, w tym najnowocześniejszych środków bezpieczeństwa i ochrony prywatności, tak aby na podstawie wszelkich danych przekazywanych EBC i krajowym bankom centralnym lub dostawcom usług wsparcia nie można było bezpośrednio zidentyfikować poszczególnych użytkowników cyfrowego euro. Aby jednak wzmocnić ten obowiązek, EROD i EIOD zalecają doprecyzowanie, że takie środki powinny zapewniać pseudonimizację danych osobowych w taki sposób, aby EBC lub krajowe banki centralne nie mogły już ich przypisać indywidualnemu użytkownikowi cyfrowego euro bez użycia dodatkowych informacji.

10.2 Artykuł 35: Przetwarzanie danych osobowych przez EBC lub krajowe banki centralne

Podstawa prawna mająca zastosowanie do przetwarzania danych przez EBC lub krajowe banki centralne

79. Artykuł 35 wniosku określa zadania, w odniesieniu do których EBC i krajowe banki centralne mogą przetwarzać dane osobowe w celu wykonania zadania „w interesie publicznym" lub w wykonywaniu „władzy publicznej". Wniosek nie zawiera jednak wyraźnego odniesienia do podstawy prawnej, na której będą się opierać w odniesieniu do przetwarzania prowadzonego do celów określonych w art. 35 ust. 1 wniosku. EROD i EIOD są zdania, że EBC i krajowe banki centralne mogą prowadzić przetwarzanie danych, o którym mowa w art. 35 ust. 1 wniosku, w interesie publicznym lub w ramach wykonywania władzy publicznej. W celu sprecyzowania podstawy prawnej przetwarzania prowadzonego przez EBC EROD i EIOD zalecają zatem współprawodawcom, aby w motywie 76 wniosku wyraźniej odnieśli się do art. 6 ust. 1 lit. e) RODO i art. 5 ust. 1 lit. a) EUDPR.

Podział obowiązków między dostawcami usług płatniczych a EBC lub krajowymi bankami centralnymi

80. EROD i EIOD uznają, że EBC lub krajowe banki centralne i dostawców usług płatniczych uważa się za odrębnych administratorów danych w przypadku przekazywania danych osobowych przez dostawców usług płatniczych do EBC lub krajowych banków centralnych w celu wykonywania zadań na podstawie art. 35 ust. 1 wniosku. Odnotowując, że użytkownicy cyfrowego euro będą wchodzić w stosunki umowne wyłącznie z dostawcami usług płatniczych (art. 13 wniosku), EROD i EIOD pragną podkreślić, że kwalifikacja ta rodzi pytanie, w jaki sposób obowiązek przejrzystości i wykonywanie praw osób, których dane dotyczą, będą zapewniane przez EBC lub krajowe banki centralne podczas przetwarzania danych osobowych do celów wymienionych w art. 35 ust. 1 projektu. W szczególności EROD i EIOD uważają, że współpraca

[76] Zob. wytyczne EROD 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego, przyjęte 7 lipca 2021 r., pkt 161–170, dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controller processor_final_en.pdf

między dostawcami usług płatniczych a EBC lub krajowymi bankami centralnymi w tym zakresie będzie miała zasadnicze znaczenie dla zapewnienia skuteczności praw osób, których dane dotyczą, zgodnie z wymogami RODO, a tym samym dla budowania wysokiego poziomu zaufania, którego oczekuje się we wniosku.

Rodzaje danych osobowych przetwarzanych przez EBC lub krajowe banki centralne

81. Artykuł 35 ust. 2 wniosku odnosi się do kategorii danych osobowych wymienionych w załączniku IV, które mogą być przetwarzane przez EBC i krajowe banki centralne w celach wymienionych w art. 35 ust. 1. Jednocześnie w załączniku IV nie wymienia się w sposób wyczerpujący rodzajów danych osobowych, które mają być przetwarzane przez EBC lub krajowe banki centralne, ale ilustruje się je w sposób niewyczerpujący przez użycie terminu „w tym". EROD i EIOD zalecają wyczerpujące wymienienie rodzajów danych osobowych zamiast używania słowa „w tym", w szczególności w przypadku:
    - pkt 1 ppkt (ii) załącznika IV, który odnosi się do przetwarzania informacji dotyczących „transakcji płatniczych w cyfrowym euro dokonywanych w trybie online"; informacji związanych „z unikatowym numerem rachunku płatniczego w cyfrowym euro, w tym kwot[y] transakcji";
    - pkt 3 załącznik IV, który odnosi się do przetwarzania „danych wymaganych do celów analizy fałszerstw w transakcjach płatniczych w cyfrowym euro dokonywanych w trybie offline: obejmuje to informacje dotyczące lokalnych urządzeń pamięciowych, w tym numer lokalnego urządzenia pamięciowego".

10.3 Artykuł 36: Przetwarzanie przez dostawców usług wsparcia

82. W art. 36 wniosku opisuje się cele, dla których przetwarzanie może być prowadzone przez dostawców usług wsparcia w sytuacji, gdy EBC postanawia powierzyć im zadanie rozwijania funkcji mechanizmu rozwiązywania sporów i zarządzania nią (art. 27 wniosku) lub zadania związane z FDPM (art. 32 wniosku).

83. Oprócz zaleceń przedstawionych już powyżej w sekcji 8.5 w odniesieniu do ogólnego FDPM, EROD i EIOD pragną zgłosić następujące uwagi dotyczące art. 36 wniosku.

Podział obowiązków pomiędzy dostawcami usług wsparcia a EBC

84. EROD i EIOD rozumieją z art. 27 ust. 2, art. 32 ust. 1 i art. 36 ust. 1 wniosku, że chociaż EBC i krajowe banki centralne będą odpowiedzialne za ustanowienie mechanizmu rozwiązywania sporów i ogólnego mechanizmu wykrywania oszustw, dostawcy usług wsparcia będą odpowiedzialni za wspieranie funkcjonowania tych mechanizmów, jeżeli EBC powierzy im to zadanie. Artykuł 36 ust. 5 wniosku przewiduje ponadto, że w przypadku udzielania takiego wsparcia dostawców usług wsparcia należy uznać za administratorów danych. W tym względzie należy pamiętać, że określenie roli administratorów w aktach legislacyjnych musi być dostosowane do faktycznych obowiązków przypisanych tym podmiotom w tych aktach

legislacyjnych[77]. EROD i EIOD uważają jednak, że wniosek w obecnym brzmieniu nie zawiera wystarczających informacji na temat faktycznych zadań, które będą wykonywane przez dostawców usług wsparcia w kontekście mechanizmu rozwiązywania sporów i ogólnego mechanizmu wykrywania oszustw, co uniemożliwia EROD i EIOD ocenę roli tych dostawców jako administratorów lub podmiotów przetwarzających podczas przetwarzania danych osobowych do celów, o których mowa w art. 36 ust. 1 wniosku. W związku z tym EROD i EIOD zalecają współprawodawcom większe doprecyzowanie obowiązków przypisanych dostawcom usług wsparcia w odniesieniu do tych mechanizmów, tak aby takie obowiązki uzasadniały rolę wspomnianych dostawców jako administratorów. Ewentualnie współprawodawców zachęca się do usunięcia z art. 36 ust. 5 kwalifikacji dostawców usług wsparcia jako administratora danych we wszystkich przypadkach, przy czym taka kwalifikacja musi zostać oceniona na późniejszym etapie w świetle faktycznych zadań powierzonych przez EBC dostawcom usług wsparcia w związku z art. 27 i 32 wniosku, a także wytycznych EROD i EIOD w sprawie pojęć administratora danych i podmiotu przetwarzającego[78].

Rodzaje danych osobowych przetwarzanych przez dostawców usług wsparcia

85. EROD i EIOD zauważają, że gdy EBC zdecyduje się powierzyć dostawcom usług wsparcia zadanie związane z ogólnym mechanizmem wykrywania oszustw i zapobiegania im, kategorie danych osobowych, o których mowa w załączniku V, byłyby bezpośrednio przekazywane tym dostawcom przez dostawców usług płatniczych na mocy art. 32 ust. 4 wniosku. EROD i EIOD zauważają jednak, że w pkt (i)–(iii) załącznika V do wniosku używa się wyrażenia „w tym" i dlatego nie zawierają one wyczerpującego wykazu rodzajów danych osobowych, a zatem zaleca się dalsze doprecyzowanie rodzaju danych osobowych, które mogłyby być przetwarzane przez dostawców usług wsparcia w ramach tych kategorii.

86. Ponadto EROD i EIOD zwracają uwagę na brak wykazu kategorii danych osobowych, które mają być przetwarzane przez dostawców usług wsparcia podczas obsługi wymiany wiadomości na potrzeby rozwiązywania sporów zgodnie z art. 27 ust. 2 wniosku, a także na brak wyjaśnienia, kto miałby przekazywać te informacje. W związku z tym EROD i EIOD zalecają dodanie tych wyjaśnień do załącznika V.

[77] Wytyczne EROD 07/2020 w sprawie pojęć administratora i podmiotu przetwarzającego, przyjęte 7 lipca 2021 r., pkt 23, dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf Wytyczne EIOD w sprawie pojęć administratora, podmiotu przetwarzającego i współadministrowania na podstawie rozporządzenia (UE) 2018/1725, przyjęte 7 listopada 2019 r., s. 8, przypis 6, dokument dostępny pod adresem: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf

[78] Wytyczne EROD 07/2020 w sprawie pojęć administratora i podmiotu przetwarzającego, przyjęte 7 lipca 2021 r., dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf; Wytyczne EIOD w sprawie pojęć administratora, podmiotu przetwarzającego i współadministrowania na podstawie rozporządzenia (UE), przyjęte 7 listopada 2019 r., dokument dostępny pod adresem: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf.

Podstawa prawna przetwarzania danych osobowych przez dostawców usług wsparcia

87. Ponadto EROD i EIOD zauważają, że wniosek nie zawiera wyraźnego odniesienia do podstawy prawnej przetwarzania danych przez dostawców usług wsparcia do celów, o których mowa w art. 36 ust. 1 wniosku. W związku z tym EROD i EIOD zalecają wyjaśnienie w motywie 76 lub art. 36 ust. 1 wniosku, że art. 6 ust. 1 lit. e) RODO miałby zastosowanie do takiego przetwarzania danych osobowych, biorąc pod uwagę, że przetwarzanie danych przez dostawców usług wsparcia będzie prowadzone w ramach zadania publicznego powierzonego im przez EBC.

11 ROZDZIAŁ IX – PRZECIWDZIAŁANIE PRANIU PIENIĘDZY

88. EROD i EIOD z zadowoleniem przyjmują fakt, że art. 37 przewiduje szczególny system stosowania przepisów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w odniesieniu do transakcji w cyfrowym euro dokonywanych w trybie offline. Takie przepisy mają na celu zapewnienie odpowiedniej równowagi między ochroną prywatności i ochroną danych osobowych z jednej strony a stosowaniem przepisów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu z drugiej strony, przy jednoczesnym uwzględnieniu szczególnego profilu ryzyka cyfrowego euro. W istocie EROD i EIOD są zdania, że obecnie obowiązujące przepisy w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu mające zastosowanie do płatności elektronicznych, umożliwiające identyfikowalność pieniądza banku komercyjnego, muszą zostać dostosowane, tak by osiągnąć cel cyfrowego euro, jakim jest zapewnienie jak najwyższego poziomu prywatności[79].

89. EROD i EIOD zauważają jednak, że w ocenie skutków wniosku[80] stwierdza się, że wariant 2e (selektywna ochrona prywatności w przypadku płatności o niskiej wartości dokonywanych w trybie online) „może być atrakcyjna dla przestępców i terrorystów", ale nie wyjaśnia się, dlaczego profil ryzyka tego wariantu byłby nieuchronnie wyższy niż profil ryzyka gotówki.

90. W tym względzie należy zauważyć, że jak przypomina Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy („FATF") w swoich zaleceniach [81], poziomu ryzyka związanego z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu nie należy określać w sposób abstrakcyjny, ale w odniesieniu do konkretnych wyborów projektowych, które zostałyby dokonane dla danej waluty cyfrowej banku centralnego („CBDC"). W tym aspekcie ocena skutków nie zawiera wystarczającej analizy profilu ryzyka cyfrowego euro związanego z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu, który to profil w praktyce zależy od stosowanych technologii i wyborów projektowych dokonanych w fazie koncepcyjnej. W związku z tym w ocenie skutków nie uwzględniono różnych profili ryzyka tego wariantu w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w tym faktu, że

[79] Oświadczenie EROD 04/2022 w sprawie wyborów projektowych dotyczących cyfrowego euro z perspektywy prywatności i ochrony danych, przyjęte 10 października 2022 r., s. 3, dokument dostępny pod adresem: https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf

[80] Strona 71 oceny skutków wniosku.

[81] FATF, *Report to the G20 Finance Ministers and Central Bank Governors on so-called Stablecoins* (Sprawozdanie dla ministrów finansów i prezesów banków centralnych państw grupy G-20 na temat tzw. stabilnych kryptowalut), czerwiec 2020 r., dokument dostępny pod adresem: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf zob. załącznik B, pkt 88, 92 i 94.

ryzyko to mogłoby zostać ograniczone przez rzeczywistą strukturę cyfrowego euro, jeżeli zostanie odpowiednio ocenione i będzie zarządzane przy zastosowaniu podejścia opartego na analizie ryzyka.

91. W szczególności EROD i EIOD uważają, że istnieje szereg środków łagodzących, które należy wziąć pod uwagę w celu zmniejszenia ryzyka związanego z przeciwdziałaniem praniu pieniędzy i finansowaniem terroryzmu i dotyczącego cyfrowego euro w trybie online. Jak podkreślono w najnowszej stosownej literaturze [82], środki takie obejmują decyzje projektowe i technologiczne, które należy podjąć na późniejszym etapie w celu zmniejszenia ryzyka związanego z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu; decyzje te dotyczą: (i) poziomu limitu utrzymywanej kwoty (ii) wprowadzenia określonego progu dla transakcji o niskiej wartości dokonywanych w trybie online, powyżej którego to progu mogą być przeprowadzane pełne kontrole, oraz (iii) możliwości ponownej identyfikacji konta użytkownika w przypadku podejrzenia. Oprócz tych środków można by dodać ograniczenia techniczne, takie jak przyjęcie odpowiedniej definicji natychmiastowości w celu uniknięcia „transakcji o wysokiej częstotliwości", ograniczenie liczby transakcji dziennie z tym samym unikatowym numerem rachunku płatniczego w cyfrowym euro lub monitorowanie wzorców finansowania i definansowania (jak ma to miejsce w przypadku trybu offline), aby zapobiec nadużyciom w stosowaniu podejścia progowego. W tym względzie EROD i EIOD zauważają, że motyw 79 wniosku wyraźnie przewiduje, że transakcje w cyfrowym euro dokonywane w trybie online mogą być obarczone niskim ryzykiem, i zakłada, że AMLA powinien określić odpowiednie „uproszczone środki należytej staranności", które dostawcy usług płatniczych powinni stosować

92. W tym względzie EROD i EIOD zauważają, że ocena skutków wniosku nie uwzględnia istnienia limitu utrzymywanej kwoty jako możliwego ograniczenia ryzyka związanego z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu w odniesieniu do cyfrowego euro w trybie online, które nie może być wykorzystywane jako środek przechowywania wartości w przeciwieństwie do pieniądza fizycznego. Ponadto w ocenie skutków nie dokonano rozróżnienia między standardowym ryzykiem związanym z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu a możliwym statusem niskiego ryzyka, co umożliwiłoby uproszczone kontrole, a tym samym przyjęcie uniwersalnego podejścia do ryzyka.

93. W związku z tym EROD i EIOD zalecają nałożenie na Eurosystem obowiązku wdrożenia najodpowiedniejszych środków technicznych w celu dalszego ograniczenia profilu ryzyka związanego z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu w odniesieniu do transakcji o niskiej wartości dokonywanych w cyfrowym euro w trybie online (na przykład przez wprowadzenie konkretnego przepisu w rozdziale X). W szczególności EROD i EIOD są zdania, że ryzyko związane z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu w przypadku transakcji o niskiej wartości dokonywanych w cyfrowym euro w trybie online powinno zostać uwzględnione i ograniczone na etapie projektowania cyfrowego euro, co byłoby bardziej odpowiednie niż ograniczenie a *priori* cech prywatności i ochrony danych w przypadku transakcji o niskiej wartości dokonywanych w cyfrowym euro w trybie online.

[82] Biały Dom, *Technical evaluation for a U.S. central bank digital currency system* (Ocena techniczna systemu waluty cyfrowej amerykańskiego banku centralnego), wrzesień 2022 r., s. 19, dokument dostępny pod adresem: https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-US-CBDC-System.pdf

Wraz z obowiązkowym przyjęciem odpowiednich środków technicznych w celu ograniczenia profilu ryzyka związanego z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu, jak zaproponowano, ograniczenie a *priori* cech prywatności i ochrony danych w odniesieniu do transakcji o niskiej wartości dokonywanych w cyfrowym euro w trybie online nie byłoby uzasadnione z technicznego punktu widzenia i nie zapewniłoby właściwej równowagi między ochroną prywatności i ochroną danych osobowych z jednej strony, a zapobieganiem praniu pieniędzy i finansowaniu terroryzmu z drugiej strony.

94. Biorąc pod uwagę wszystkie te względy, EROD i EIOD wyrażają ubolewanie, że we wniosku odrzucono „selektywne podejście do prywatności" w odniesieniu do płatności w cyfrowym euro dokonywanych w trybie online, które było rozważane przez sam EBC[83]. Konkretniej rzecz ujmując, EROD i EIOD zalecają, aby szczególny system, który miałby zastosowanie do trybu offline (i dotyczyłby kontroli w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu wyłącznie w odniesieniu do finansowania i definansowania), został rozszerzony na tryb online dla transakcji o niskiej wartości, i w ten sposób ustanowiono by próg prywatności, czyli próg, poniżej którego nie występuje śledzenie transakcji do celów przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Próg ten można ustanowić w drodze aktu wykonawczego zgodnie z procedurą określoną w art. 37 ust. 5 i 6 wniosku, na podstawie wcześniejszej oceny ryzyka obejmującej zarówno ryzyko w zakresie ochrony danych, jak i zagrożenia związane z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu. W celu uproszczenia i zwiększenia efektywności próg ten może być taki sam jak limit transakcji dla trybu offline, obejmujący w szczególności codzienne transakcje o niskiej wartości[84].

95. Ponadto, w odniesieniu do określenia „limitu transakcji" dla trybu offline, EROD i EIOD przypominają o potrzebie znalezienia właściwej równowagi między zapobieganiem ryzyku związanemu z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu z jednej strony a zachowaniem prawa do ochrony danych i prywatności z drugiej strony. Powinno to znaleźć odzwierciedlenie w art. 37 wniosku. W szczególności EROD i EIOD zauważają, że kryteria, które

[83] Na przykład w niedawnym przemówieniu do komisji ECON Fabio Panetta, członek Rady Wykonawczej EBC, oświadczył, komentując poziom ryzyka płatności o niższej wartości: „[o]gólnie rzecz biorąc, można rozważyć większy stopień prywatności w przypadku płatności o niższej wartości dokonywanych w trybie online i offline. Płatności te mogłyby podlegać uproszczonym kontrolom w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, natomiast transakcje o wyższej wartości nadal podlegałyby standardowym kontrolom". Zob.: EBC, Oświadczenie wprowadzające Fabia Panetty, członka Zarządu EBC, na posiedzeniu Komisji Gospodarczej i Monetarnej Parlamentu Europejskiego, 30 marca 2022 r., dokument dostępny pod adresem: https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220330_1~f9fa9a6137.en.html

[84] EROD i EIOD zauważają, że takie wielopoziomowe podejście (z brakiem kontroli lub ograniczonymi kontrolami dla transakcji o niskiej wartości dokonywanych w trybie online) jest coraz bardziej powszechne w projektach cyfrowej waluty banku centralnego (CBDC) na całym świecie. Jak stwierdzono/odnotowano w niedawnym dokumencie informacyjnym MFW, „[...] *we wszystkich trzech aktywnych projektach CBDC wybrano taki sam sposób postępowania w odniesieniu do kompromisu między anonimowością / integracją finansową a przestrzeganiem przepisów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Ich podejście polegało na zapewnieniu wielostopniowego wyboru portfeli o różnych poziomach progów. Te o niższych progach umożliwiają większą anonimowość. (...) Korzystanie z wielopoziomowych portfeli CBDC prowadzi zatem do »synergii polityki« między anonimowością, ograniczeniem ryzyka (paniki bankowej) i włączeniem finansowym"*. Zob.: Międzynarodowy Fundusz Walutowy, *Behind the scenes of central bank digital currency: emerging trends, insights and, policy lessons* (Za kulisami cyfrowej waluty banku centralnego: nowe trendy, spostrzeżenia i wnioski polityczne), luty 2022 r., s. 13, dokument dostępny pod adresem: https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022004.ashx.

Komisja ma wziąć pod uwagę w art. 37 ust. 6 przy podejmowaniu decyzji w sprawie limitów transakcji i utrzymywanych kwot dla trybu offline, są związane z ryzykiem przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oraz zapewnieniem „wykorzystania i akceptowania" cyfrowego euro, ale nadal brakuje odniesienia do prywatności płatności. Jest to zaskakujące z punktu widzenia ochrony danych, ponieważ ochrona prywatności jest jednym z głównych celów tego trybu. EROD i EIOD zalecają zatem, aby art. 37 ust. 6 wniosku odnosił się do skutków w zakresie prywatności i ochrony danych osobowych.

96. Co więcej, EROD i EIOD zauważają, że art. 37 ust. 6 wniosku przewiduje jedynie, że Komisja „może" skonsultować się z EROD przy uchwalaniu aktu delegowanego w tej sprawie. Nie jest jednak jasne, czy i w jaki sposób konsultacje te miałyby się odbyć. Wniosek powinien przewidywać ustrukturyzowany i zinstytucjonalizowany mechanizm, a nie tylko możliwość konsultacji z EROD. W związku z tym EROD i EIOD zalecają współprawodawcom wprowadzenie na końcu art. 37 ust. 6 obowiązku ścisłej współpracy z AMLA i formalnych konsultacji z EROD przy wydawaniu opinii wymaganej przez Komisję (jak zaproponowano w opinii EIOD w odniesieniu do art. 7 ust. 4 wniosku dotyczącego rozporządzenia w sprawie ram dostępu do danych finansowych[85]) oraz uwzględnienia tej opinii przez Komisję przed przedstawieniem projektu aktu delegowanego. Pozostawałoby to bez uszczerbku dla konsultacji z EIOD zgodnie z EUDPR.

97. Wreszcie niektóre przepisy tego artykułu wymagają doprecyzowania, aby uniknąć jakichkolwiek wątpliwości co do znaczenia prywatności i ochrony danych osobowych w odniesieniu do trybu offline. W szczególności:

- EROD i EIOD zalecają zapewnienie spójności między art. 37 ust. 2, który stanowi, że dostawcy usług płatniczych, EBC ani krajowe banki centralne nie mogą zachowywać danych dotyczących transakcji, a pkt 3 załącznika IV, który stanowi, że Eurosystem może odczytywać wszystkie informacje na lokalnym urządzeniu pamięciowym „do celów analizy fałszerstw w transakcjach płatniczych w cyfrowym euro dokonywanych w trybie offline";
- W art. 37 ust. 2 termin „zachowywać" [dane dotyczące transakcji] jest niejasny z punktu widzenia ochrony danych, ponieważ można by było oczekiwać terminu „przetwarzać" lub „uzyskiwać dostęp". „Zachowywać" wydaje się sugerować, że dane mogą być dostępne, co nie spełnia poziomu prywatności, do którego dąży się w trybie offline. EROD i EIOD zalecają zatem zastąpienie słowa „zachowywać" słowem „przetwarzać";
- Artykuł 37 ust. 4 zawiera wśród „danych dotyczących finansowania i definansowania", które mają być przetwarzane do celów przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, identyfikator lokalnego urządzenia pamięciowego na potrzeby płatności w cyfrowym euro dokonywanych w trybie offline. W związku z tym EROD i EIOD zalecają wyjaśnienie powodów konieczności przetwarzania takiej kategorii danych do celów art. 37 ust. 3, biorąc pod uwagę, że wniosek przewiduje już przetwarzanie innych kategorii danych osobowych, w tym numeru rachunku wykorzystywanego (numerów rachunków wykorzystywanych) do finansowania i definansowania;

[85] Opinia EIOD nr 38/2023 w sprawie wniosku dotyczącego rozporządzenia w sprawie ram dostępu do danych finansowych, przyjęta 22 sierpnia 2023 r., pkt 30, dokument dostępny pod adresem: https://edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf

98. Wreszcie EROD i EIOD zauważają, że zgodnie z art. 35 ust. 4 w związku z motywem 76 wniosku należy stosować wyraźną segregację danych osobowych, aby Eurosystem nie mógł bezpośrednio zidentyfikować poszczególnych użytkowników cyfrowego euro. W tym względzie EROD i EIOD zalecają wprowadzenie obowiązku zapewnienia przez Eurosystem segregacji danych w lokalnym urządzeniu pamięciowym w odniesieniu do transakcji dokonywanych w trybie offline i transakcji o niskiej wartości dokonywanych w trybie online. We wniosku należy wskazać, że dane dotyczące transakcji powinny być „wyodrębnione" (tzn. znajdować się w lokalnym urządzeniu pamięciowym) i nie powinny być eksportowane poza to urządzenie (dane są przetwarzane i przechowywane lokalnie). Z technicznego punktu widzenia możliwe jest wdrożenie i uruchomienie tej segregacji, co ostatecznie zapewni użytkownikom silniejsze zabezpieczenia w odniesieniu do ustawień prywatności w przypadku korzystania z cyfrowego euro w trybie offline.

12 ROZDZIAŁ X – PRZEPISY KOŃCOWE

99. EROD i EIOD zauważają, że w art. 38 wniosku Komisję upoważnia się do zmiany załączników w drodze aktów delegowanych. W tym względzie, biorąc pod uwagę spodziewany znaczący wpływ na poziom prywatności i ochrony danych osobowych zainteresowanych osób, EROD i EIOD zalecają wprowadzenie wyraźnego odniesienia do art. 42 EUDPR, aby wyjaśnić, że gdy proponowane są takie akty delegowane, należy, w stosownych przypadkach, konsultować się z EIOD lub EROD.

100. Jeżeli chodzi o przegląd rozporządzenia na podstawie art. 41 wniosku, prywatność i ochrona danych powinny być centralnym aspektem, który Komisja powinna ocenić w swoich sprawozdaniach. EROD i EIOD pozostają do dyspozycji w celu dostarczania Komisji istotnych informacji podczas przygotowywania tych sprawozdań, które mają być przedstawiane po upływie roku od pierwszej emisji cyfrowego euro, a następnie co trzy lata[86].

UWAGI KOŃCOWE

101. Podczas gdy proces legislacyjny UE jest w toku, Rada Prezesów EBC przeprowadzi jesienią 2023 r. przegląd wyników etapu badania i na tej podstawie zdecyduje, czy rozpocząć bardziej eksperymentalny etap cyfrowego euro, z ambicją wyemitowania cyfrowego euro w ciągu dwóch lub trzech lat [87]. W tym kontekście EROD i EIOD przypominają o obowiązku przeprowadzenia oceny skutków dla ochrony danych przez wszystkich administratorów i współadministratorów danych związanych z cyfrowym euro w zakresie, w jakim spełnione są wymogi określone w art. 35 RODO lub art. 39 EUDPR dotyczące przeprowadzenia takiej oceny, przy czym najlepiej byłoby taką ocenę opublikować.

[86] Artykuł 41 ust. 1 wniosku.
[87] EBC, *Progress on the investigation phase of a digital euro – fourth report* (Postępy na etapie badania cyfrowego euro – czwarte sprawozdanie), 14 lipca 2023 r., dokument dostępny pod adresem: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews230714.en.html#:~:text=The%20fourth%20progress%20report%20on,it%20could%20strengthen%20financial%20inclusion.

102. EBC powinien również ocenić potrzebę zasięgnięcia opinii EIOD przed przeprowadzeniem przetwarzania w odniesieniu do cyfrowego euro, ponieważ takie przetwarzanie prawdopodobnie spowodowałoby wysokie ryzyko naruszenia praw i wolności osób fizycznych. W szczególności przetwarzanie danych osobowych przez EBC spełniałoby co najmniej trzy kryteria określone w wytycznych EROD dotyczących oceny skutków dla ochrony danych (np. ocena lub punktacja w kontekście FDPM, przetwarzanie danych wrażliwych w zakresie, w jakim odnosi się ono do finansów użytkowników cyfrowego euro, oraz przetwarzanie na dużą skalę)[88].

103. W tym kontekście EROD i EIOD zalecają, aby we wniosku przypomniano o spoczywającym na EBC obowiązku przeprowadzenia oceny skutków dla ochrony danych i powierzono EBC zadanie zapewnienia cyfrowego euro z wbudowaną zgodnością z obowiązkiem uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych na kolejnych etapach projektu, takich jak przyjęcie wyborów technologicznych, zasad systemowych i weryfikacja poprawności projektu. Taki przepis wyraźnie zapewniłby obywatelom przejrzystość w zakresie zabezpieczeń wprowadzonych w celu osiągnięcia cyfrowego euro, które skutecznie chroni ich prywatność i dane osobowe. Powyższe można na przykład wprowadzić w art. 36a lub w przepisach końcowych (rozdział X).

W imieniu Europejskiego Inspektora Ochrony Danych

Europejski Inspektor Ochrony Danych

(Wojciech Wiewiórowski)

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Anu Talus)

[88] Wytyczne Grupy Roboczej art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, przyjęte 4 kwietnia 2017 r., s. 9–11, dokument dostępny pod adresem: https://ec.europa.eu/newsroom/article29/items/611236/en