POLSKA ORGANIZACJA NIEBANKOWYCH INSTYTUCJI PŁATNOŚCI

ul. Ogrodowa 58,
00-807 Warszawa

NIP: 7010297287
REGON: 142934847

22 398 16 50
kontakt@ponip.pl
www.ponip.pl

STANOWISKO DOTYCZĄCE INTERPRETACJI PRZEPISÓW DORA W ASPEKCIE USŁUG ICT ORAZ ZDU ICT

Niniejsze stanowisko interpretacyjne zostało wypracowane w trakcie spotkań, konsultacji i debat w gronie kilkudziesięciu przedstawicieli i ekspertów grupy roboczej ds. interpretacji przepisów DORA („**Grupa Robocza**"), powołanej w ramach Polskiej Organizacji Niebankowych Instytucji Płatności („**PONIP**"). Prace grupy były koordynowane oraz wspierane prawnie przez prawników Kancelarii ftl.

Celem niniejszego dokumentu jest przedstawienie odpowiedzi na wątpliwości interpretacyjne związane ze stosowaniem DORA w ramach procesów, polityk oraz modeli biznesowych rynku usług płatniczych oraz fintech. W niniejszym dokumencie analizie poddane zostały kluczowe obszary oddziaływania DORA na ten rynek oraz przedstawione zostały wytyczne w zakresie stosowania regulacji DORA, będące przedmiotem prac Grupy Roboczej.

Warszawa, 6 lutego 2025 roku

I. Zakres i cel dokumentu

1. Od dnia 17 stycznia 2025 roku podmioty finansowe mają obowiązek stosowania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego. W związku z m.in. wysokim stopniem skomplikowania tego aktu prawnego (łącznie z wydanymi na jego podstawie aktami wykonawczymi oraz delegowanymi), małą precyzją stosowanych w nim sformułowań (w tym w ramach definicji), relatywnie krótkim okresem obowiązywania oraz przede wszystkim skromną liczbą wypowiedzi właściwych organów czy doktryny (w szczególności wytycznych interpretacyjnych przedstawionych przez unijne i polskie organy), interpretacja przepisów DORA może budzić istotne wątpliwości. W związku z tym w ramach PONIP została powołana grupa robocza, której zadaniem było zidentyfikowanie problemów oraz uzgodnienie jednolitej interpretacji przepisów DORA poprzez opracowanie wspólnego stanowiska w tej materii.
2. Przedstawione w niniejszym stanowisku wytyczne interpretacyjne zostały sformułowane na podstawie informacji dostępnych członkom Grupy Roboczej na moment ich przyjmowania. Nie można wykluczyć, iż w czasie dalszego obowiązywania przepisów DORA mogą zaistnieć okoliczności wpływające na treść przyjętych wytycznych, w szczególności w przypadku wydania przez organy nadzoru stanowisk lub komunikatów odnoszących się do sposobu rozumienia przez te organy poszczególnych norm prawnych. Niniejsze stanowisko może więc wymagać w przyszłości aktualizacji lub rozszerzenia, a zawarte w niniejszym stanowisku wytyczne interpretacyjne powinny być na bieżąco monitorowane pod kątem ich aktualności.
3. Dokument nie stanowi opinii prawnej ani stanowiska żadnego z poszczególnych członków Grupy Roboczej. Decyzja co do konkretnego kształtu wdrożenia przepisów DORA pozostaje w każdym przypadku w wyłącznej kompetencji poszczególnych podmiotów finansowych.

II. Użyte skróty

API PSD2	Interfejsy posiadane przez ASPSP na potrzeby umożliwienia świadczenia usług przez TPP.
ASPSP	Podmioty finansowe będące dostawcami świadczącymi usługę prowadzenia rachunków płatniczych dostępnych on-line.
DORA	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.
ITS-R	Rozporządzenie wykonawcze Komisji (UE) 2024/2956 z dnia 29 listopada 2024 r. ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych wzorów na potrzeby rejestru informacji.
PSD2	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
Podwykonawcy ICT	Zewnętrzni dostawcy Usług ICT ZDU ICT w ramach tego samego łańcucha dostaw Usług ICT.
RTS-SC	Final report on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554 (JC 2023 67).
RTS SCA	Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji.
TPP	Dostawcy świadczący usługę dostępu do informacji o rachunku oraz dostawcy świadczący usługę inicjowania transakcji płatniczej.

Usługi ICT	Usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego, łącznie ze sprzętem komputerowym jako usługą i usługami w zakresie sprzętu komputerowego obejmującymi zapewnianie wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu, z wyłączeniem tradycyjnych usług telefonii analogowej (art. 3 pkt 21 DORA).
UUP	Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych.
ZDU ICT	Zewnętrzni dostawcy Usług ICT.

III. Treść stanowiska

III.1. Usługa rachunku bankowego

Usługa rachunku bankowego nie stanowi Usługi ICT w rozumieniu DORA.

- Pojęcie Usługi ICT na podstawie samej definicji zawartej w art. 3 pkt 21 DORA ma szeroki zakres znaczeniowy i wymaga doprecyzowania (interpretacji) w sposób odzwierciedlający cel DORA. Nadrzędnym celem DORA jest osiągnięcie odporności cyfrowej, a także sprawne świadczenie usług finansowych. Nieuzasadnione wydaje się rozciąganie reżimu DORA na usługi, które – choć czysto literalnie mogłyby wpisywać się w definicję Usługi ICT - to mają dla podmiotu finansowego mocno pomocniczy charakter i bez których świadczenie usług finansowych oraz działalność podmiotu finansowego nie uległyby znaczącej zmianie.
- Rachunki bankowe świadczone dla instytucji płatniczej służą przede wszystkim bieżącemu funkcjonowaniu instytucji płatniczej jako przedsiębiorcy. Rachunek bankowy, oferowany przez banki bądź instytucje kredytowe, jest usługą finansową, do której świadczenia niezbędne jest uzyskanie zezwolenia wydanego przez właściwe organy. Jednocześnie banki podlegają ścisłemu nadzorowi organów i zobowiązane są do przestrzegania znacznie bardziej rygorystycznych wymogów dotyczących bezpieczeństwa ICT, w tym wynikających z DORA, niż te nałożone przez DORA na ZDU ICT. Europejskie Urzędy Nadzoru (Europejski Urząd Nadzoru Bankowego, Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych oraz Europejski Urząd Nadzoru Giełd i Papierów Wartościowych) wskazywały w swoich wypowiedziach, że niecelowym byłoby nakładanie na podmiot finansowy współpracujący z innym podmiotem dodatkowych wymogów, które są konsumowane przez wymogi, do których podmiot finansowy ma obowiązek się dostosować ze względu na samą swoją działalność.
- Stanowisko to zostało formalnie potwierdzone przez Europejskie Urzędy Nadzoru, o czym szerzej mowa w pkt III.11 niniejszego dokumentu. Wobec tego za uzasadnione należy uznać wyłączenie z pojęcia Usług ICT usług świadczonych przez podmioty finansowe, mające co prawda charakter technologiczny, jednak świadczone jako immanentna i naturalna część usługi finansowej świadczonej przez te podmioty. Usługi te są już objęte nadzorem właściwych organów oraz wymogami mającymi na celu zapewnienie ich bezpieczeństwa.
- Ponadto należy zauważyć, że rachunek bankowy jako usługa nie spełnia definicji Usługi ICT według DORA: sama w sobie nie jest usługą cyfrową ani też usługą w zakresie danych. Podstawową usługą świadczoną przez bank na rzecz instytucji płatniczych jest właśnie usługa rachunku bankowego, nie zaś usługa technologiczna, która może towarzyszyć prowadzeniu rachunku płatniczego (która sama w sobie nie jest ani usługą cyfrową ani usługą w zakresie danych). Stąd nie należy traktować usługi prowadzenia rachunku bankowego jako Usługi ICT w rozumieniu DORA.
- Istotne jest wyraźne oddzielenie samej natury (podstawy) usługi od środków, za pośrednictwem których usługa ta jest świadczona. Jaskrawy przykład to np. subskrypcja prasy za pomocą Internetu – naturą usługi jest udostępnienie odbiorcy zbioru tekstów, co do niedawna odbywało się wyłącznie w formie papierowej, nie jest to więc usługa cyfrowa ani też usługa w zakresie danych – nie kwalifikuje się zatem jako Usługa ICT. Dopiero środki komunikacji, za pomocą których usługa ta jest świadczona to systemy ICT, jednak nie powinno to wpływać na wynik kwalifikacji samej usługi subskrypcji prasy.

III.2. Bankowość internetowa oraz usługi typu connect

Usługa bankowości internetowej oraz usługi typu connect nie stanowią Usług ICT w rozumieniu DORA.

- Usługa connect oraz usługa bankowości elektronicznej mają charakter czysto pomocniczy do podstawowej, biznesowej usługi jaką jest utrzymywanie rachunku bankowego. Również z punktu widzenia świadczenia usług płatniczych są to elementy pomocnicze, udostępniane dodatkowo, a wykonanie usługi płatniczej nie jest od nich zależne ani bezpośrednio z nimi powiązane. Dostawca usług płatniczych wykonuje usługę płatniczą bez ścisłego powiązania z umową connect lub bankowości internetowej. W tym rozumieniu uznanie ich za Usługi ICT w rozumieniu DORA jest zbyt daleko idące.
- Bankowość internetowa jest funkcjonalnością udostępnianą przez banki, w celu umożliwienia klientowi korzystania z rachunku bankowego, w szczególności zlecania transakcji płatniczych w ciężar tego rachunku oraz uzyskiwania podglądu środków zgromadzonych na rachunku. Usługa bankowości internetowej nie stanowi samodzielnej usługi technologicznej – jej świadczenie w oderwaniu od rachunku bankowego nie jest możliwe. Usługa ta stanowi tym samym *de facto* część usługi finansowej rachunku bankowego.
- Niedostępność usługi bankowości internetowej nie ma żadnego wpływu na świadczenie usług płatniczych ani inne obszary działalności instytucji płatniczej.
- Celem DORA jest osiągniecie operacyjnej odporności cyfrowej podmiotów finansowych. Objęcie omawianej usługi bankowości internetowej reżimem DORA nie podniesie poziomu odporności cyfrowej podmiotu finansowego, z kolei brak objęcia tej usługi reżimem DORA nie będzie miał negatywnych skutków w tym zakresie.
- Usługą ICT jest **wyłącznie usługa cyfrowa** bądź **usługa w zakresie danych**. Szereg usług, które same w sobie nie są usługą cyfrową ani usługą w zakresie danych będzie w jakimś stopniu świadczona za pośrednictwem systemów ICT (np. w zakresie przekazywania raportów i informacji dotyczących wykonania usługi), jednak sama forma dostarczania usługi nie przesądza o uznaniu jej za Usługę ICT.
- Europejskie Urzędy Nadzoru wskazywały w swoich wypowiedziach, że niecelowym byłoby nakładanie na bank współpracujący z innym podmiotem dodatkowych wymogów, które są konsumowane przez wymogi, do których bank musi się dostosować ze względu na samą swoją działalność. Stanowisko to zostało formalnie potwierdzone przez Europejskie Urzędy Nadzoru, o czym szerzej mowa w pkt III.11 niniejszego dokumentu. Wobec tego za uzasadnione należy uznać wyłączenie z pojęcia Usług ICT usług świadczonych przez podmioty finansowe, mające co prawda charakter technologiczny, jednak świadczone jako immanentna i naturalna część usługi finansowej świadczonej przez te podmioty. Usługi te są już objęte nadzorem właściwych organów oraz wymogami mającymi na celu zapewnienie ich bezpieczeństwa.
- Powyższe uwagi w takim samym stopniu należy odnieść do usług typu connect, zapewniających spersonalizowany dostęp dla podmiotu do prowadzonych na jego rzecz rachunków bankowych.
- Również więc w odniesieniu do bankowości internetowej oraz usług typu connect należy stwierdzić, że nie stanowią one Usługi ICT w rozumieniu DORA.
- Powyższe nie wpływa przy tym na fakt, że podmioty finansowe mogą stanowić jednocześnie ZDU ICT i świadczyć na rzecz innych podmiotów finansowych usługi ICT. Takie podejście potwierdzają zarówno motywy DORA, jak również wypowiedzi Europejskich Urzędów Nadzoru, które sugerują, że usługi infrastruktury finansowej, takie jak VISA i MasterCard, należy uznać za usługi ICT. Nie powinno to jednak dotyczyć usług świadczonych jako immanentna i naturalna część usługi finansowej.

III.3. API PSD2

Udostępnienia przez ASPSP API PSD2 nie stanowi świadczenia przez ASPSP Usług ICT na rzecz TPP.

- ASPSP są obowiązane do posiadania API PSD2 na potrzeby umożliwienia świadczenia usług przez TPP. Zasady udostępniania API PSD2 oraz korzystania z nich podlegają ścisłej regulacji przez przepisy UUP oraz RTS SCA (art. 30 i nast. RTS SCA), które przewidują między innymi obowiązek ASPSP do zapewnienia zgodności API PSD2 ze standardami komunikacji publikowanymi przez międzynarodowe lub europejskie organy normalizacyjne.

- Pomimo niewątpliwie technicznego charakteru interfejsów udostępnianych przez te podmioty finansowe, ich udostępnianie stanowi wykonanie ich obowiązku wynikającego z powszechnie obowiązujących przepisów prawa. Zgodnie z art. 59r ust. 5 oraz 59s ust. 4 UUP, korzystanie przez użytkownika z usług TPP nie może być uzależnione od istnienia stosunku umownego między TPP a ASPSP. Nie sposób więc uznać, że ASPSP świadczy na rzecz TPP jakiekolwiek Usługi ICT w rozumieniu DORA, bowiem pomiędzy tymi podmiotami nie występuje relacja usługodawca – usługobiorca, a jedynie TPP wykorzystuje mechanizm, który jest mu udostępniany na mocy przepisów. Dodatkowo ze względu na brak relacji umownej między ASPSP a TPP nie jest możliwe spełnienie wymogów DORA dotyczących minimalnej treści umowy między podmiotem finansowym a ZDU ICT. TPP, korzystający z API PSD2 na potrzeby świadczonych przez siebie dla użytkowników usług, nie ma jakichkolwiek uprawnień kontraktowych do domagania się od dostawcy prowadzącego rachunek zapewnienia odpowiedniego API PSD2. W żaden sposób nieuzasadnione byłoby natomiast twierdzenie, że z przepisów DORA wynika konieczność zawarcia pomiędzy ASPSP a TPP odpowiedniej umowy wbrew normie art. 59r ust. 5 i 59s ust. 4 UUP, w szczególności ze względu na fakt, że taka konkluzja zaprzeczyłaby sensowi regulacji UUP w zakresie zasad otwartej bankowości.
- Należy zauważyć, że API PSD2 utrzymywane według standardu Polish API spełnia wymogi PSD2 oraz RTS SCA. Niecelowym byłoby nakładanie na podmioty stosujące ten standard dodatkowych obowiązków wynikających z DORA, bo doprowadziłoby to do powielenia zabezpieczeń i środków, które zostały już określone w innych aktach prawa unijnego jako specyficzne dla API PSD2.
- Należy więc opowiedzieć się za uznaniem, że zapewnienie API PSD2 zgodnie z wymogami przepisów prawa, w szczególności w oparciu o standard Polish API, nie stanowi świadczenia Usługi ICT w rozumieniu DORA na rzecz innych podmiotów finansowych.
- Odmiennej oceny wymagałby przypadek, gdyby API PSD2 byłoby udostępniane na podstawie umowy zawartej pomiędzy TPP a ASPSP.

III.4. Pay-by-link

Usługi komunikacji pay-by-link nie stanowią Usługi ICT w rozumieniu DORA.

- W ramach świadczenia przez agentów rozliczeniowych tzw. usług pay-by-link (usług polegających na przyjmowaniu płatności z wykorzystaniem przelewów zlecanych w uproszczony sposób za pośrednictwem bankowości internetowej, bez ręcznego wprowadzania danych o transakcji i odbiorcy) zazwyczaj dostawca prowadzący rachunek bankowy oraz acquierer świadczący usługę pay-by-link ustalają określone zasady komunikacji, pozwalające na przekazywanie pomiędzy tymi podmiotami informacji w związku ze zlecaniem płatności, w szczególności dostawca prowadzący rachunek udostępnia agentowi rozliczeniowemu interfejs komunikacyjny na potrzeby przekazywania informacji („Usługi komunikacji pay-by-link").
- Usługa komunikacji pay-by-link jest świadczona na podstawie umowy pomiędzy agentem rozliczeniowym oraz dostawcą prowadzącym rachunek i zazwyczaj połączona jest z umową o świadczenie dla agenta rozliczeniowego usługi rachunku płatniczego. Usługa ma na celu jedynie umożliwienie złożenia w uproszczony sposób zlecenia płatniczego i istnieje w ścisłym powiązaniu z umową rachunku. Komunikat przekazywany w ramach Usługi komunikacji pay-by-link nie funkcjonowałaby bez usługi prowadzenia rachunku. Z tego względu dostawca usługi prowadzenia rachunku nie świadczy usługi Komunikacji pay-by-link jako ZDU ICT, a jedynie umożliwia przekazywanie komunikatów związanych zainicjowaniem transakcji płatniczej z tego rachunku w ramach swojej działalności jako podmiotu finansowego.
- W taki sam sposób należy ocenić sytuację, kiedy z Usługi komunikacji pay-by-link korzysta dostawca usług płatniczych w celu świadczenia swoich usług płatniczych. Także w takim przypadku Usługa komunikacji pay-by-link jest ściśle powiązana z usługą płatniczą i ma na celu umożliwienie złożenia zlecenia płatniczego w uproszczony, szybszy sposób. Ma ona charakter czysto pomocniczy, dodatkowy do podstawowej, biznesowej usługi płatniczej. Nie stanowi samodzielnej usługi technicznej.
- Europejskie Urzędy Nadzoru wskazywały w swoich wypowiedziach, że niecelowym byłoby nakładanie na bank współpracujący z innym podmiotem dodatkowych wymogów, które są konsumowane przez wymogi, do których bank ma się dostosować ze względu na samą swoją działalność. Stanowisko to zostało formalnie potwierdzone

przez Europejskie Urzędy Nadzoru, o czym szerzej mowa w pkt III.11 niniejszego dokumentu. Wobec tego za uzasadnione należy uznać wyłączenie z pojęcia Usług ICT usług świadczonych przez podmioty finansowe, mające co prawda charakter techniczny, jednak świadczone jako immanentna i naturalna część usługi finansowej świadczonej przez te podmioty. Usługi te są już objęte nadzorem właściwych organów oraz wymogami mającymi na celu zapewnienie ich bezpieczeństwa.

- Powyższe uwagi w takim samym stopniu należy odnieść do Usługi komunikacji pay-by-link świadczonej przez banki prowadzące rachunki bankowe, jak również w sytuacji, w której Usługa pay-by-link jest ściśle powiązana z usługą płatniczą świadczoną przez dostawcę usług płatniczych.
- Również więc w odniesieniu do Usług komunikacji pay-by-link, świadczonych we wskazanych powyżej okolicznościach, należy stwierdzić, że nie stanowią one Usługi ICT w rozumieniu DORA.
- Z uwagi na różnorodne modele Usług komunikacji pay-by-link oraz treść umów, na podstawie których są świadczone, nie można jednak wykluczyć, że w danych okolicznościach podmiot finansowy zakwalifikuje te usługi jako Usługi ICT w rozumieniu DORA, a podmioty, które je świadczą, jako ZDU ICT. Ocena w tym zakresie powinna zostać dokonana przez poszczególne podmioty finansowe na podstawie konkretnych warunków, na jakich Usługa komunikacji pay-by-link jest im świadczona, z uwzględnieniem ryzyka związanego z ICT, które ona może generować.

III.5. Podpis elektroniczny

Podpis elektroniczny nie stanowi Usług ICT.

- Usługa kwalifikowanego podpisu elektronicznego wykorzystywana jest powszechnie przez osoby fizyczne stanowiące personel podmiotów finansowych, w ramach wykonywania obowiązków wobec tych podmiotów, jako ich pracownicy, współpracownicy oraz członkowie organów.
- Pomimo wykorzystania tych narzędzi w ramach działalności podmiotów finansowych, same podmioty finansowe nie są stronami umów o ich dostarczenie – z dostawcami podpisów umowy posiadają każdorazowo właściwe osoby fizyczne.
- Tym samym uzasadnione jest przyjęcie, że usługę kwalifikowanego podpisu elektronicznego dla personelu podmiotu finansowego nie należy uznać za Usługę ICT świadczoną na rzecz podmiotu finansowego.

III.6. Usługi świadczone na rzecz hybrydowych instytucji płatniczych

Usługi wspierające prowadzenie przez hybrydową instytucję płatniczą „innej działalności gospodarczej", o której mowa w art. 74 ust. 1 pkt 3 UUP, nie stanowią Usług ICT w rozumieniu DORA, jeżeli nie mają wpływu na bezpieczeństwo świadczonych usług płatniczych.

- Zakres zastosowania DORA obejmuje również hybrydowe instytucje płatnicze, zdefiniowane w art. 2 pkt 9 UUP jako instytucje płatnicze wykonujące oprócz usług płatniczych, wydawania pieniądza elektronicznego lub działalności, o której mowa w art. 74 ust. 1 pkt 1 i 2 oraz ust. 3 UUP, także inną działalność gospodarczą. Działalność prowadzoną przez hybrydowe instytucje płatnicze można zatem w uproszczony sposób podzielić na:
  - działalność płatniczą,
  - procesy wspierające wyłącznie inną działalność gospodarczą (niepodlegającą obowiązkowi uzyskania wpisu do rejestru bądź zezwolenia).
- Należy opowiedzieć się za uznaniem, że za ZDU ICT nie należy uznawać dostawców świadczących dla hybrydowej instytucji płatniczej usługi, które wspierają wyłącznie jej „inną działalność gospodarczą", zgodnie z podziałem wskazanym powyżej, i nie mają wpływu na bezpieczeństwo ICT w zakresie usług płatniczych, w szczególności dotyczą działalności odseparowanej systemowo od działalności płatniczej.
- Za wykładnią taką przemawia przede wszystkim zakres stosowania DORA określony w art. 2 ust. 1 i 2 DORA. Przepis ten wprowadza zamknięty katalog rodzajów podmiotów finansowych objętych DORA. Oznacza to, że podmioty, które nie zostały ujęte w tym katalogu, nie są obowiązane stosować przepisów DORA, a prowadzona przez nie działalność nie została objęta ochroną określoną w DORA. Jeżeli zatem hybrydowa instytucja płatnicza prowadzi

działalność, która nie byłaby objęta zakresem zastosowania DORA, gdyby była prowadzona przez podmiot niebędący podmiotem finansowym, to takie same zasady powinny dotyczyć tej działalności w przypadku wykonywania jej przez hybrydową instytucję płatniczą. Wniosek taki potwierdza motyw 63 preambuły DORA, który odwołuje się wprost do rozwiązań technologicznych „umożliwiających sprawne świadczenie **usług finansowych**".

- Interpretację tę potwierdza także wzór rejestru informacji o ZDU ICT oraz instrukcja wypełniania go zawarta w ITS-R. Dokumenty te przewidują obowiązki podmiotów finansowych w zakresie wskazywania funkcji wyznaczonych wewnętrznie i przypisanie każdej z tych funkcji do rodzaju licencjonowanej lub rejestrowanej działalności, określonych w art. 2 ust. 1 DORA. W przypadku określenia przez podmiot finansowy funkcji, której nie da się przypisać do żadnej działalności licencjonowanej czy rejestrowanej, ITS-R przewiduje dodatkowo możliwość opisania jej ręcznie jako „*support functions*" (funkcje wspierające).
- ITS-R nie odnoszą się natomiast do funkcji, które wyznaczone byłyby w ramach „innej działalności gospodarczej", która w żaden sposób nie wspiera i nie dotyka obszaru działalności płatniczej i z tego względu nie można jej uznać za „funkcję wspierającą". Wynika z tego, że postanowienia umowne dotyczące wyłącznie „innej działalności gospodarczej" nie powinny być raportowane w ramach rejestru informacji, a co za tym idzie, że zamysłem prawodawcy nie było objęcie DORA całego tego obszaru.

III.7. Podwykonawstwo zlecone przez ZDU ICT niewspierającego krytycznych lub istotnych funkcji

Wymogi dotyczące podwykonawców ICT, o których mowa w art. 30 ust. 2 lit. a DORA, odnoszą się wyłącznie do podwykonawstwa zleconego przez ZDU ICT wspierającego krytyczne lub istotne funkcje.

- DORA wprowadza obowiązek wskazania w ustaleniach umownych dotyczących korzystania z Usług ICT, czy dozwolone jest podwykonawstwo Usługi ICT wspierającej krytyczną lub istotną funkcję lub jej istotnych części, a jeżeli tak, to jakie warunki mają zastosowanie do takiego podwykonawstwa.
- Chociaż obowiązek ten został określony w ramach wskazania ogólnych wymogów dla umowy podmiotu finansowego z ZDU ICT (tj. w ramach art. 30 ust. 2 DORA odnoszącego się do wszystkich umów z ZDU ICT, nie zaś w ramach art. 30 ust. 3 DORA odnoszącego się jedynie do umów z ZDU wspierających krytyczne lub istotne funkcje), to literalne brzmienie art. 30 ust. 2 lit a DORA oraz całokształt treści RTS-SC, który wydany został w celu doprecyzowania normy art. 30 ust. 2 lit a, pozwala twierdzić, że wymogi, o których mowa w tym przepisie, odnoszą się jedynie do podwykonawców ZDU ICT wspierających funkcje istotne lub krytyczne (co najmniej istotną część funkcji krytycznej lub istotnej wspieranej przez ZDU).
- W szczególności przepisy RTS-SC odnoszą się jedynie do takiego przypadku, co potwierdza także tytuł tego aktu prawnego jednoznacznie wskazujący na uregulowanie w nim elementów, które podmiot finansowy musi określić i ocenić w przypadku zlecania podwykonawstwa Usług ICT wspierających **funkcje krytyczne lub istotne**.
- Jednoznacznie wynika to także z treści art. 30 ust. 5 DORA zawierającego upoważnienie dla Europejskich Urzędów Nadzoru do opracowania, za pośrednictwem Wspólnego Komitetu, projektu regulacyjnych standardów technicznych doprecyzowujących elementy, o których mowa w art. 30 ust. 2 lit. a) DORA, które podmiot finansowy musi określić i ocenić, zlecając podwykonawstwo usług ICT wspierających **krytyczne lub istotne funkcje**.
- Fakt umieszczenia wspomnianego postanowienia w ust. 1 (odnoszącym się także do ZDU ICT niewspierających funkcji krytycznych lub istotnych) można potraktować jako odniesienie do sytuacji, w której dany ZDU ICT świadczy wiele usług ICT, z których tylko niektóre wspierają krytyczne lub istotne funkcje.
- Pomimo odrzucenia przez Komisję Europejską ostatecznego projektu RTS-SC, którego tekst stanowił podstawę do przedstawienia powyższej argumentacji, jej zasadność nie budzi wątpliwości, a ewentualne zmiany w treści RTS-SC nie powinny wpłynąć na brzmienie przedstawionych powyżej wniosków. Po przyjęciu finalnego brzmienia rozporządzenia delegowanego ustanawiającego regulacyjne standardy techniczne w przedmiotowej materii, konieczna może być weryfikacja przedstawionej argumentacji w celu jej ewentualnej aktualizacji, uwzględniającej literalne brzmienie przyjętego rozporządzenia.

III.8. Podmioty wykonujące czynności niestanowiące same w sobie Usług ICT, ale będące częścią Usługi ICT

Zakresem pojęcia Podwykonawcy ICT nie jest objęty podmiot, który wykonuje na rzecz ZDU ICT czynności, które same w sobie nie stanowią Usług ICT.

- W zależności od sposobu i zakresu definiowania Usługi ICT, niektóre usługi, niestanowiące same w sobie Usługi ICT, mogą być niezbędne w celu zapewnienia prawidłowego wykonania Usługi ICT przez ZDU ICT.
- Uzasadnione jest przyjęcie węższego zakresu rozumienia Podwykonawców ICT w zakresie rodzaju świadczonych przez nich usług, tzn. przyjęcie, że pojęciem Podwykonawcy ICT powinni być objęci jedynie usługodawcy świadczący sami w sobie „mikro" Usługę ICT w rozumieniu DORA oraz ITS-R.
- Przemawia za tym zasadnicza konstrukcja RTS-SC, gdzie co do zasady mowa jest o Podwykonawcy ICT, jako podmiocie, w odniesieniu do którego ZDU ICT powinien zrealizować określone obowiązki, co wskazuje na to, że Podwykonawca ICT również powinien wykonywać Usługi ICT.
- Potwierdza to również motyw 3 RTS-SC, gdzie wskazano, że celem RTS-SC jest uregulowanie przypadków korzystania przez ZDU ICT z innych ZDU ICT, będących w takim przypadku Podwykonawcami ICT.
- Należy zauważyć, że na gruncie przepisów DORA, w szczególności definicji Usługi ICT, należy odróżnić samą Usługę ICT od funkcji krytycznej lub istotnej, którą ta usługa wspiera. O ile w realizację powierzonej podwykonawcy funkcji może być zaangażowany usługodawca nieświadczący Usługi ICT, o tyle w ramach Usługi ICT wspierającej daną funkcję powinno się wyróżniać jedynie mniejsze, częściowe Usługi ICT.
- W związku z powyższym uzasadnione jest przyjęcie, że zakresem pojęcia Podwykonawcy ICT nie jest objęty podmiot, który wykonuje na rzecz ZDU ICT czynności, które same w sobie nie stanowią Usług ICT.

III.9. Informacje o poszczególnych podmiotach z łańcucha dostaw

Podmiot finansowy może zobowiązać ZDU ICT do przekazywania mu informacji o Podwykonawcach ICT w ramach łańcucha dostaw.

- Artykuł 3 ust. 2 lit b ITS-R nakłada na podmioty finansowe obowiązek zapewnienia, aby w prowadzonym przez nie rejestrze informacji rejestru informacji o wszystkich ustaleniach umownych dotyczących korzystania z usług ICT świadczonych przez ZDU ICT, znajdowały się informacje o wszystkich Podwykonawcach ICT, którzy efektywnie wspierają świadczenie Usługi ICT wspierającej krytyczną lub istotną funkcję lub jej istotną część.
- Zakres pojęcia Podwykonawcy ICT rozciąga się zatem w zakresie tego obowiązku również na dalszych podwykonawców ZDU ICT, którzy nie posiadają bezpośredniej relacji umownej z ZDU ICT, a jedynie z Podwykonawcami ICT. Tego typu informacje o związku usług świadczonych przez danego Podwykonawcę ICT z pierwotną Usługą ICT oraz o stopniu ich wpływu na Usługę ICT może realnie posiadać ZDU ICT lub jego kolejni Podwykonawcy ICT, których łączą umowy z ich Podwykonawcami ICT, a nie podmiot finansowy.
- Podmiot finansowy powinien dołożyć należytej staranności w uzyskaniu i zweryfikowaniu informacji o Podwykonawcach ICT w ramach łańcucha dostaw, w szczególności poprzez zobowiązanie ZDU ICT do przekazywania odpowiednich informacji o całym łańcuchu outsourcingowym, w tym także wskazania jego Podwykonawców ICT mających realny wpływ na Usługę ICT wraz z wymogiem nałożenia przez ZDU ICT w umowach z jego Podwykonawcami ICT obowiązków umożliwiających ZDU ICT wykonanie przedmiotowego obowiązku wobec podmiotu finansowego.

III.10. Alternatywne poziomy zabezpieczeń

Określone w art. 30 ust. 3 lit. e pkt ii) DORA prawo należy interpretować jako uprawnienie do uzgodnienia alternatywnych (innych rodzajowo) poziomów zabezpieczenia (właściwego wykonywania Usług ICT przez ZDU ICT) w przypadku naruszenia praw innych klientów ZDU ICT wskutek realizacji uprawnień kontrolnych podmiotu finansowego np. wskutek dostępu do informacji, dokumentacji lub systemów.

- Art. 30 ust. 3 lit. e DORA wskazuje na konieczność zawarcia w umowie o świadczenie Usług ICT prawa do monitorowania ZDU ICT przez podmiot finansowy. Prawo to obejmuje: (i) nieograniczone prawa dostępu, kontroli i audytu przez podmiot finansowy, (ii) prawo do uzgodnienia alternatywnych poziomów zabezpieczenia w przypadku naruszenia praw innych klientów, (iii) obowiązek ZDU ICT do pełnej współpracy podczas kontroli i audytów, (iv) obowiązek przekazywania szczegółowych informacji na temat zakresu, mających zastosowanie procedur i częstotliwości takich kontroli i audytów.
- Określone w podpunkcie ii) prawo do uzgodnienia alternatywnych poziomów zabezpieczenia w przypadku naruszenia praw innych klientów zostało sformułowane w sposób mogący wzbudzać wątpliwości co do jego

znaczenia. Należy je jednak interpretować jako uprawnienie do uzgodnienia alternatywnych (innych rodzajowo) poziomów zabezpieczenia (właściwego wykonywania Usług ICT przez ZDU ICT) w przypadku naruszenia praw innych klientów ZDU ICT wskutek realizacji uprawnień kontrolnych podmiotu finansowego, np. wskutek dostępu do informacji, dokumentacji lub systemów.

- Możliwość ograniczenia, w sytuacji wskazanej w przepisie, prawa audytu, kontroli, inspekcji dostawcy przez podmiot finansowy potwierdzają wytyczne niemieckiego organu nadzoru (BaFin), który w ramach swoich wyjaśnień dot. stosowania DORA (Guidance notes on the implementation of DORA for ICT risk management and ICT third-party risk management[1]), podsumowując poszczególne klauzule umowne wynikające z DORA, w odniesieniu do art. 30 ust. 3 lit. e ppkt ii DORA wskazał, że odpowiednia klauzula w tym zakresie powinna określać: „Restriction of audit rights in case of rights of other customers are affected".
- Podobne stanowisko wyraził austriacki organ nadzoru finansowego w zamieszczonej na jego stronie internetowej sekcji dotyczącej DORA „Questions and Answers"[2]. Organ ten na pytanie o to, co oznacza termin „assurance levels" i jak należy rozumieć prawo do ustalenia „alternative assurnace levels" wskazał, że w przypadku, gdy „tradycyjne" uprawnienia do kontroli/audytu naruszałyby prawa innych klientów dostawcy ze względu na konkretną sytuację, można uzgodnić alternatywne sposoby monitorowania usług dostawcy.
- Takie rozumienie możliwości uzgadniania „poziomów zabezpieczeń" (level of assurance) zostało potwierdzone już w przeszłości, podczas prac nad Wytycznymi EBA w sprawie outsourcingu (EBA/GL/2019/02, Guidelines on outsourcing arrangements)[3]. EBA w finalnym raporcie dotyczącym konsultacji przedmiotowych wytycznych wskazał przykładowo, w jakich przypadkach może nastąpić ograniczenie prawa audytu dostawcy i kiedy „alternative ways to provide a similar level of assurance" powinno nastąpić[4]. Zgodnie z przedmiotowym raportem, jeśli podmiot finansowy audytuje, kontroluje u dostawcy środowiska IT, gdzie znajdują się dane wielu różnych klientów dostawcy, wtedy podmiot finansowy musi postępować z ostrożnością, żeby unikać lub mitygować ryzyka dla środowisk IT innych klientów dostawcy (np. wpływ na obniżenie SLA czy dostępność i poufność danych innych klientów dostawcy).
- Należy zauważyć, że wątpliwości interpretacyjne art. 30 ust. 3 lit. e pkt ii DORA są spowodowane brzmieniem tłumaczenia przedmiotowego przepisu na język polski. Polski termin „alternatywne poziomy zabezpieczeń" w wersji angielskiej DORA to „alternative assurance levels", co należy interpretować jako „alternatywne poziomy zapewnienia/pewności/gwarancji" informacji i danych udostępnianych podmiotowi finansowemu przez dostawcę w związku z brakiem możliwości audytu, kontroli, inspekcji dostawcy ze względu na potencjalne naruszenie danych innych klientów dostawcy. Te alternatywne poziomy pewności mają wskazywać na inne metody weryfikacji informacji dostawcy. Często w terminologii angielskiej (np. w ramach badania/audytów sprawozdań finansowych) stosowany jest termin „reasonable level of assurance" oznaczający rozsądny poziom pewności/gwarancji badanej materii. Niezależny audyt przeprowadzony przez zewnętrznego audytora klasyfikowany jest jako przykład zapewniający najwyższy „poziom pewności/gwarancji" badanej materii, porównywalny z audytem samego podmiotu finansowego. Następnie można wymienić przeglądy, audyty wewnętrzne, samooceny dostawcy, badania ankietowe, raporty/zestawienie informacji, danych przygotowanych przez dostawcę czy prezentacja procedur, polityk, dokumentacji dostawcy jak dany obszar funkcjonuje, które mogą być przykładami innych mechanizmów dających niższy poziom pewności i weryfikacji badanej materii niż audyt.
- Mając na uwadze powyższe, nie sposób się zgodzić z ewentualnymi interpretacjami, zgodnie z którymi sformułowanie „w przypadku naruszenia praw innych klientów" należałoby rozumieć jako okoliczność oderwaną od audytów przeprowadzanych przez podmiot finansowy, aktualizującą jego prawo do stosowania wobec ZDU ICT dodatkowych wymogów, mających przeciwdziałać dalszym naruszeniom.

[1] https://www.bafin.de/SharedDocs/Downloads/EN/Anlage/dl_2024_07_08_Aufsichtsmitteilung_Umsetzungshinweise_DORA_en.html (dostęp: 06.02.2025 r.).

[2] https://www.fma.gv.at/en/cross-sectoral-topics/dora/dora-managing-of-ict-third-party-risk/ (dostęp: 06.02.2025 r.).

[3] https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf, s. 117. Uwagi zgłaszane do paragrafu 79 (dostęp: 06.02.2025).

[4] Aktualne brzmienie pkt 96 Wytycznych: Podczas przeprowadzania audytów w środowiskach wielu klientów należy dołożyć starań w celu uniknięcia powstania zagrożeń dla środowiska innego klienta (np. wpływu na gwarantowane poziomy usług, dostępność danych, aspekty poufności) lub ograniczenia takich zagrożeń.

III.11. Podmioty finansowe a ZDU ICT

Podmioty finansowe, w zakresie, w jakim świadczą na rzecz innych podmiotów finansowych usługi płatnicze wymagające uzyskania zezwolenia lub wpisu do rejestru, nie są ZDU ICT.

- Usługi płatnicze mogą być świadczone wyłącznie przez podmioty spełniające wymagania określone w UUP (w przypadku instytucji płatniczych – przez posiadające zezwolenie wydane przez Komisję Nadzoru Finansowego). Uzyskanie zezwolenia na świadczenia usług płatniczych w charakterze instytucji płatniczej wymaga m.in. zapewnienia przez podmiot ubiegający się o to zezwolenie ostrożnego i stabilnego zarządzania działalnością objętą wnioskiem o wydanie zezwolenia, w szczególności przez posiadanie systemu zarządzania ryzykiem i kontroli wewnętrznej odpowiedniego do rodzaju, skali i stopnia złożoności świadczonych usług płatniczych.
- Podmioty finansowe wskazane w art. 2 ust. 1 DORA mają obowiązek stosowania DORA i podlegają w tym zakresie nadzorowi sprawowanemu przez właściwe organy. Obowiązki nałożone przez DORA na podmioty finansowe są przy tym szersze niż te, które powinny spełniać ZDU ICT. Dodatkowo, co istotne – o ile nad przestrzeganiem DORA przez podmioty finansowe nadzór sprawuje bezpośrednio właściwy organ, o tyle spełnianie tych wymogów przez ZDU ICT powinno wynikać z obowiązków nałożonych na te podmioty w umowach z podmiotami finansowymi, na rzecz których świadczą Usługi ICT. Dostawca Usług ICT, jeżeli nie świadczy ich na rzecz podmiotu finansowego, nie jest zobowiązany do przestrzegania wymogów wynikających z DORA. Zostaje objęty pośrednio przepisami tego aktu prawnego w konsekwencji zawarcia umowy z podmiotem finansowym i świadczenia na rzecz podmiotu finansowego Usług ICT. Jego obowiązki w tym zakresie są zatem niejako „wtórne" względem obowiązków samego podmiotu finansowego.
- Z powyższego wynika, że krajowa instytucja płatnicza, która świadczyłaby usługi na rzecz innego podmiotu finansowego w zakresie, w którym usługi te wymagają uzyskania zezwolenia KNF, w pierwszej kolejności jest zobowiązana do stosowania DORA z uwagi na swój status podmiotu finansowego (jest to obowiązek „pierwotny" wynikający wprost z przepisów samego DORA), a postanowienia umowy z podmiotem finansowym, na rzecz którego świadczy te usługi, wprowadzałyby obowiązek stosowania DORA niejako „wtórnie", zobowiązując taką krajową instytucję płatniczą do wypełniania obowiązków, które i tak – i to w szerszym zakresie – byłaby zobowiązana do stosowania na podstawie samego DORA. Nawet gdyby podmiot finansowy nie nałożył w zawartej z taką instytucją płatniczą w umowie obowiązków wynikających z DORA, instytucja płatnicza i tak byłaby zobowiązana do ich przestrzegania, a co więcej – spełnienie tego obowiązku podlegałoby nadzorowi KNF. Wskazane powyżej wnioski dotyczą usług świadczonych przez krajową instytucję płatniczą jedynie w zakresie, w jakim usługi te są objęte zezwoleniem KNF. W tym bowiem jedynie zakresie instytucja płatnicza ma obowiązek stosować DORA jako podmiot finansowy i podlega nadzorowi KNF co do stosowania się do przepisów rozporządzania.
- Także Europejskie Urzędy Nadzoru wskazywały w swoich wypowiedziach, że niecelowym byłoby nakładanie na podmiot finansowy współpracujący z innym podmiotem dodatkowych wymogów, które są konsumowane przez wymogi, do których podmiot finansowy ma obowiązek się dostosować ze względu na samą swoją działalność[5]. W jednym ze stanowiska wskazano: „*W przypadku, gdy podmiot finansowy jest dostawcą usług, (…) w przypadku których podmiot finansowy musi być upoważniony/licencjonowany/zarejestrowany jako podmiot finansowy do ich świadczenia, takie usługi są zatem regulowanymi usługami finansowymi, a nie usługami ICT w rozumieniu art. 3(21) DORA. Podmioty finansowe będą musiały dokonać własnej oceny*".
- Europejskie Urzędu Nadzoru, we współpracy z Komisją Europejską, formalnie potwierdziły swoje stanowisko co do interpretacji Usługi ICT, udzielając odpowiedzi na pytanie co do tego, jakie typy usług powinny być uznawane za Usługi ICT[6]. W odpowiedzi tej wskazano, że w przypadku, gdy podmioty finansowe świadczą Usługi ICT na rzecz innych podmiotów finansowych w związku ze świadczonymi przez nie usługami finansowymi, podmioty finansowe, na rzecz których te usługi są świadczone, powinny ocenić, czy i) usługi stanowią Usługi ICT oraz ii) czy świadczące te usługi podmioty finansowe i usługi finansowe, które świadczą, są regulowane na mocy prawa Unii Europejskiej lub dowolnego ustawodawstwa krajowego państwa członkowskiego lub państwa trzeciego. Jeżeli oba testy

[5] https://www.eba.europa.eu/sites/default/files/2024-05/0af21cec-b473-4906-b9cc-878675875c2d/DORA%20Dry%20Run%20FAQ.pdf (dostęp: 06.02.2025 r.).

[6] https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/2999-dora030_en (dostęp: 06.02.2025 r.).

wypadną pozytywnie, powiązaną Usługę ICT należy uznać przede wszystkim za usługę finansową i nie należy jej traktować jako Usługi ICT w rozumieniu art. 3 pkt 21 DORA. W przypadku jednak, gdy Usługa ICT nie jest powiązana z usługą finansową, usługę tę należy uznać za Usługę ICT w rozumieniu art. 3 pkt 21 DORA.

- Powyższe wnioski, zgodnie ze stanowiskiem Europejskich Urzędów Nadzoru przytoczonym powyżej, nie znajdą zastosowania do sytuacji, w której instytucja płatnicza świadczy na rzecz podmiotu finansowego inne usługi, nie będące usługami płatniczymi. Oznacza to, że jeżeli instytucja płatnicza świadczy dla podmiotu finansowego Usługi ICT, które z racji swojej istoty nie są objęte zezwoleniem KNF, nie świadczy ich w charakterze podmiotu finansowego, a zewnętrznego dostawcy Usług ICT. Obowiązek stosowania DORA powinien w takiej sytuacji w odniesieniu do tych usług zostać na nią nałożony w umowie o świadczenie Usług ICT zawartej z podmiotem finansowym. Nadzór nad wypełnianiem wymogów wynikających z DORA nałożonych na nią w umowie należy w takiej sytuacji także do podmiotu finansowego.
- Konieczność traktowania instytucji płatniczej jako ZDU ICT w sytuacji, w której świadczy na rzecz podmiotu finansowego usługi nieobjęte zezwoleniem KNF potwierdza motyw nr 63 do preambuły DORA. Motyw ten stanowi, że instytucje finansowe, w tym instytucje płatnicze, powinny być uznane za dostawcę ICT w zakresie, w jakim świadczą Usługi ICT dla innych instytucji finansowych. Chodzi tu o sytuacje, kiedy instytucja płatnicza świadczy usługi o charakterze technicznym, a nie bezpośrednio usługi płatnicze lub usługi bezpośrednio związane/powiązane ze świadczeniem usług płatniczych przez tę instytucję płatniczą. Usługi te, o charakterze technicznym, powiązane z płatnościami, określono w treści motywu jako „rozwiązania związane z płatnościami", a podmioty świadczące takie usługi jako „uczestników ekosystemu usług płatniczych prowadzący działania przetwarzania płatności lub obsługujący infrastrukturę płatniczą". Tego rodzaju podmioty należy odróżniać od podmiotów finansowych świadczących stricte usługi płatnicze.