Wytyczne 6/2020 w sprawie wzajemnych zależności między dyrektywą PSD2 a RODO

Wersja 2.0

przyjęte 15 grudnia 2020 r.

Historia wersji

Wersja 2.0	15.12.2020 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	17.07.2020 r.	Przyjęcie wytycznych do konsultacji w sprawie publikacji

Spis treści

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

a także mając na uwadze, co następuje:

(1) Ogólne rozporządzenie o ochronie danych przewiduje spójny zestaw przepisów dotyczących przetwarzania danych osobowych w całej UE.

(2) Drugą dyrektywą w sprawie usług płatniczych (dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r., zwana dalej „PSD2") uchylono dyrektywę 2007/64/WE i ustanowiono nowe przepisy mające na celu zapewnienie pewności prawa konsumentom, akceptantom i przedsiębiorstwom w łańcuchu płatności oraz modernizację ram prawnych dla rynku usług płatniczych[2]. Państwa członkowskie miały dokonać transpozycji PSD2 do prawa krajowego przed dniem 13 stycznia 2018 r.

(3) Ważną cechą PSD2 jest wprowadzenie ram prawnych dla nowych usług inicjowania płatności i usług dostępu do informacji o rachunku. PSD2 umożliwia dostawcom tych nowych usług płatniczych uzyskanie dostępu do rachunków płatniczych osób, których dane dotyczą, w celu świadczenia wspomnianych usług.

(4) Jeżeli chodzi o ochronę danych, zgodnie z art. 94 ust. 1 PSD2 wszelkie przetwarzanie danych osobowych, w tym przekazywanie informacji o przetwarzaniu, na potrzeby PSD2 odbywa się zgodnie z RODO[3] oraz z rozporządzeniem (UE) 2018/1725.

(5) Motyw 89 PSD2 stanowi, że w przypadku przetwarzania danych osobowych do celów PSD2 należy określić dokładny cel, przywołać stosowną podstawę prawną, spełnić stosowne wymogi dotyczące bezpieczeństwa ustanowione w RODO, a także przestrzegać zasad konieczności, proporcjonalności, ograniczenia celu oraz proporcjonalnego okresu zatrzymywania danych. Ponadto uwzględnienie ochrony danych już w fazie projektowania i domyślna ochrona danych powinny być wbudowane we wszystkie systemy przetwarzania danych opracowywane i używane w ramach PSD2[4].

(6) Motyw 93 PSD2 stanowi, że dostawcy świadczący usługę inicjowania płatności i dostawcy świadczący usługę dostępu do informacji o rachunku, z jednej strony, oraz dostawca usług płatniczych prowadzący rachunek, z drugiej strony, powinni przestrzegać niezbędnych wymogów w zakresie

[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Motyw 6 PSD2.
[3] W związku z tym, że PSD2 powstała przed RODO, nadal zawiera odniesienia do dyrektywy 95/46/WE. Art. 94 RODO stanowi, że odesłania do uchylonej dyrektywy 95/46/EW należy traktować jako odesłania do RODO.
[4] Motyw 89 PSD2.

ochrony danych i bezpieczeństwa, które zostały określone lub o których mowa w niniejszej dyrektywie lub które uwzględniono w regulacyjnych standardach technicznych.

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1. WPROWADZENIE

1. Druga dyrektywa w sprawie usług płatniczych (dalej jako: „PSD2") wprowadziła szereg nowości w obszarze usług płatniczych. Chociaż stwarza ona nowe możliwości dla konsumentów i zwiększa przejrzystość w tym obszarze, stosowanie PSD2 rodzi pewne pytania i obawy związane z koniecznością zachowania przez osoby, których dane dotyczą, pełnej kontroli nad własnymi danymi osobowymi. Ogólne rozporządzenie o ochronie danych (zwane dalej „RODO") ma zastosowanie do przetwarzania danych osobowych, w tym do czynności przetwarzania dokonywanych w kontekście usług płatniczych, określonych w PSD2[5]. W związku z tym administratorzy działający w obszarze objętym PSD2 muszą zawsze zapewniać zgodność z wymogami RODO, w tym z zasadami ochrony danych określonymi w art. 5 RODO, jak również z odpowiednimi przepisami dyrektywy o prywatności i łączności elektronicznej[6]. Chociaż PSD2[7] oraz regulacyjne standardy techniczne dotyczące silnego uwierzytelniania klienta oraz wspólnych i bezpiecznych otwartych standardów komunikacji (zwane dalej „regulacyjnymi standardami technicznymi"[8]) zawierają określone przepisy dotyczące ochrony i bezpieczeństwa danych, pojawiła się niepewność co do interpretacji tych przepisów, jak również wzajemnych zależności między ogólnymi ramami ochrony danych a PSD2.

2. 5 lipca 2018 r. EROD wydała pismo dotyczące PSD2, w którym udzieliła wyjaśnień w kwestiach dotyczących ochrony danych osobowych w związku z tą dyrektywą, w szczególności w zakresie przetwarzania danych osobowych nieumawiających się stron (tzw. danych milczącej strony) przez dostawców świadczących usługę dostępu do informacji o rachunku oraz dostawców świadczących usługę inicjowania płatności, procedur dotyczących wyrażania i wycofywania zgody, regulacyjnych standardów technicznych oraz współpracy pomiędzy dostawcami usług płatniczych prowadzącymi rachunek w odniesieniu do środków bezpieczeństwa. Z kolei prace przygotowawcze nad niniejszymi wytycznymi obejmowały zebranie uwag od zainteresowanych stron, zarówno w formie pisemnej, jak i podczas spotkania z zainteresowanymi stronami, w celu określenia najpilniejszych wyzwań.

3. Niniejsze wytyczne służą zapewnieniu dalszych wskazówek dotyczących aspektów ochrony danych w kontekście PSD2, w szczególności powiązań między odpowiednimi przepisami RODO i PSD2. Największy nacisk w wytycznych położono na przetwarzanie danych osobowych przez dostawców

[5] Art. 1 ust. 1 RODO.

[6] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej); Dz.U. L 201 z 31.7.2002, s. 37.

[7] Art. 94 PSD2 itp.

[8] 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 (Tekst mający znaczenie dla EOG.); C/2017/7782; Dz.U. L 69 z 13.3.2018, s. 23-43; dostępne pod adresem https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018R0389&from=EN

świadczących usługę dostępu do informacji o rachunku oraz dostawców świadczących usługę inicjowania płatności. W związku z tym niniejszy dokument dotyczy warunków udzielania dostępu do informacji o rachunku płatniczym przez dostawców usług płatniczych prowadzących rachunek oraz przetwarzania danych osobowych przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku, w tym wymogów i środków ochronnych w odniesieniu do przetwarzania danych osobowych przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku w celach innych niż pierwotne cele, dla których zgromadzono dane, w szczególności gdy zgromadzono je w kontekście świadczenia usługi dostępu do informacji o rachunku[9]. W niniejszym dokumencie odniesiono się również do odmiennych pojęć wyraźnej zgody na podstawie PSD2 i RODO, przetwarzania „danych milczącej strony", przetwarzania szczególnych kategorii danych osobowych przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku, stosowania głównych zasad ochrony danych określonych w RODO, w tym minimalizacji danych, przejrzystości, rozliczalności i środków bezpieczeństwa. PSD2 obejmuje wielofunkcyjne obowiązki m.in. w obszarze ochrony konsumentów i prawa konkurencji. Rozważania dotyczące wspomnianych dziedzin prawa wykraczają poza zakres niniejszych wytycznych.

4. Aby ułatwić lekturę wytycznych, poniżej podano główne definicje stosowane w niniejszym dokumencie.

1.1 Definicje

„Dostawca świadczący usługę dostępu do informacji o rachunku" oznacza dostawcę usługi online polegającej na dostarczaniu skonsolidowanych informacji na temat co najmniej jednego rachunku płatniczego posiadanego przez danego użytkownika usług płatniczych u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych;

„dostawca usług płatniczych prowadzący rachunek" oznacza dostawcę usług płatniczych zapewniającego i utrzymującego rachunek płatniczy dla płatnika;

„minimalizacja danych" jest zasadą ochrony danych, zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

„płatnik" oznacza osobę fizyczną lub prawną, która jest posiadaczem rachunku płatniczego i zezwala na wykonanie zlecenia płatniczego z tego rachunku płatniczego, lub w przypadku gdy rachunek płatniczy nie istnieje – osobę fizyczną lub prawną, która składa zlecenie płatnicze;

„odbiorca" oznacza osobę fizyczną lub prawną będącą zamierzonym odbiorcą środków pieniężnych, które są przedmiotem transakcji płatniczej;

„rachunek płatniczy" oznacza rachunek prowadzony w imieniu co najmniej jednego użytkownika usług płatniczych, wykorzystywany do wykonywania transakcji płatniczych;

„dostawca świadczący usługę inicjowania płatności" oznacza dostawcę świadczącego usługę polegającą na zainicjowaniu zlecenia płatniczego na wniosek użytkownika usług płatniczych w odniesieniu do rachunku płatniczego posiadanego u innego dostawcy usług płatniczych;

[9] Usługa dostępu do informacji o rachunku to usługa online polegająca na dostarczaniu skonsolidowanych informacji na temat co najmniej jednego rachunku płatniczego posiadanego przez danego użytkownika usług płatniczych u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych.

„dostawca usług płatniczych" oznacza podmiot, o którym mowa w art. 1 ust. 1 PSD2[10], lub osobę fizyczną lub prawną korzystającą ze zwolnienia na podstawie art. 32 lub 33 PSD2;

„użytkownik usług płatniczych" oznacza osobę fizyczną lub prawną korzystającą z usługi płatniczej w charakterze płatnika, odbiorcy lub płatnika i odbiorcy;

„dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

„uwzględnianie ochrony danych w fazie projektowania" odnosi się do środków technicznych i organizacyjnych wbudowanych w produkt lub usługę, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych oraz włączenia do procesu przetwarzania niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą;

„domyślna ochrona danych" oznacza odpowiednie środki techniczne i organizacyjne wdrożone w ramach produktu lub usługi, które służą zapewnieniu, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania;

„regulacyjny standard techniczny" oznacza rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę (UE) 2015/2366 Parlamentu Europejskiego i Rady w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji;

„dostawcy usług będący osobami trzecimi" oznacza zarówno dostawców świadczących usługę inicjowania płatności, jak i dostawców świadczących usługę dostępu do informacji o rachunku.

1.2 Usługi, o których mowa w PSD2

5. W PSD2 wprowadzono dwa nowe typy (dostawców) usług płatniczych: dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku. Załącznik I do PSD2 zawiera osiem usług płatniczych objętych tą dyrektywą.

[10] Art. 1 ust. 1 PSD2 stanowi, że dyrektywa ta ustanawia przepisy, zgodnie z którymi państwa członkowskie rozróżniają następujące kategorie *dostawców usług płatniczych*:
a) instytucje kredytowe zgodnie z definicją w art. 4 ust. 1 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 (1), w tym ich oddziały w rozumieniu art. 4 ust. 1 pkt 17 tego rozporządzenia, gdy takie oddziały znajdują się w Unii, bez względu na to, czy siedziby zarządu tych oddziałów znajdują się w Unii, czy – zgodnie z art. 47 dyrektywy 2013/36/UE i prawem krajowym – poza Unią;
b) instytucje pieniądza elektronicznego w rozumieniu art. 2 pkt 1 dyrektywy 2009/110/WE, w tym – zgodnie z art. 8 tej dyrektywy i prawem krajowym – ich oddziały, gdy takie oddziały znajdują się w Unii, a ich siedziby zarządu znajdują się poza Unią, o ile usługi płatnicze świadczone przez te oddziały są związane z emisją pieniądza elektronicznego;
c) instytucje świadczące żyro pocztowe, które są na mocy prawa krajowego uprawnione do świadczenia usług płatniczych;
d) instytucje płatnicze;
e) EBC i krajowe banki centralne, gdy nie działają one w charakterze organów kształtujących politykę pieniężną lub innych organów publicznych;
f) państwa członkowskie lub ich władze regionalne lub lokalne, gdy nie działają one w charakterze organów publicznych.

6. Dostawcy świadczący usługę inicjowania płatności świadczą usługi polegające na inicjowaniu zleceń płatniczych na wniosek użytkownika usług płatniczych w odniesieniu do rachunku płatniczego użytkownika posiadanego u innego dostawcy usług płatniczych[11]. Dostawca świadczący usługę inicjowania płatności może zwrócić się do dostawcy usług płatniczych prowadzącego rachunek (zazwyczaj banku) o zainicjowanie transakcji w imieniu użytkownika usług płatniczych. Użytkownikiem (usług płatniczych) może być osoba fizyczna (osoba, której dane dotyczą) lub osoba prawna.

7. Dostawcy świadczący usługę dostępu do informacji o rachunku świadczą usługę online polegającą na dostarczaniu skonsolidowanych informacji na temat co najmniej jednego rachunku płatniczego posiadanego przez danego użytkownika usług płatniczych u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych[12]. Zgodnie z motywem 28 PSD2 użytkownik usług płatniczych ma możliwość uzyskania w danym momencie natychmiastowego ogólnego obrazu swojej sytuacji finansowej.

8. Jeżeli chodzi o usługi dostępu do informacji o rachunku, może istnieć kilka różnych rodzajów oferowanych usług, z naciskiem na różne funkcje i cele. Na przykład niektórzy dostawcy mogą oferować użytkownikom usługi, takie jak planowanie budżetu i monitorowanie wydatków. Przetwarzanie danych osobowych w kontekście tych usług podlega PSD2. Usługi, które wiążą się z oceną zdolności kredytowej użytkownika usług płatniczych, lub usługi audytu świadczone poprzez gromadzenie informacji za pośrednictwem usługi dostępu do informacji o rachunku, nie wchodzą w zakres PSD2, a zatem podlegają RODO. Ponadto PSD2 nie obejmuje również rachunków innych niż rachunki płatnicze (np. oszczędnościowych, inwestycyjnych). W każdym przypadku RODO stanowi obowiązujące ramy prawne dla przetwarzania danych osobowych.

Przykład 1:

HappyPayments to spółka, która oferuje usługę online polegającą na udostępnianiu informacji o co najmniej jednym rachunku płatniczym za pośrednictwem aplikacji mobilnej w celu monitorowania finansów (usługa dostępu do informacji o rachunku). Dzięki tej usłudze użytkownik usług płatniczych może natychmiast zobaczyć salda i ostatnie transakcje na co najmniej dwóch rachunkach płatniczych w różnych bankach. Na życzenie użytkownika usług płatniczych oferuje ona również klasyfikację wydatków i dochodów według różnych typologii (wynagrodzenie, wypoczynek, energia, kredyt hipoteczny itp.), pomagając w ten sposób użytkownikowi usług płatniczych w zakresie planowania finansowego. W ramach wspomnianej aplikacji HappyPayments oferuje również usługę inicjowania płatności bezpośrednio ze wskazanych przez użytkownika rachunków płatniczych (usługa inicjowania płatności).

9. Z myślą o świadczeniu tych usług w PSD2 uregulowano warunki prawne, na jakich dostawcy świadczący usługę inicjowania płatności i dostawcy świadczący usługę dostępu do informacji o rachunku mogą uzyskiwać dostęp do rachunków płatniczych w celu świadczenia usługi na rzecz użytkownika usług płatniczych.

10. Art. 66 ust. 1 i art. 67 ust. 1 PSD2 stanowią, że użytkownik usług płatniczych ma prawo dostępu do usług płatniczych i usług dostępu do informacji o rachunku oraz prawo do korzystania z tych usług. Oznacza to, że użytkownik usług płatniczych powinien zachować całkowitą swobodę w korzystaniu z tego prawa i nie może być zmuszany do korzystania z niego.

[11] Art. 4 pkt 15 PSD2.
[12] Art. 4 pkt 16 PSD2.

11. Dostęp do rachunków płatniczych i korzystanie z informacji o rachunkach płatniczych uregulowano częściowo w art. 66 i 67 PSD2, zawierających środki ochronne odnoszące się do ochrony danych (osobowych). Art. 66 ust. 3 lit. f) PSD2 stanowi, że dostawca świadczący usługę inicjowania płatności nie żąda od użytkownika usług płatniczych żadnych danych innych niż dane niezbędne do wykonania usługi inicjowania płatności, a art. 66 ust. 3 lit. g) tej dyrektywy stanowi, że dostawcy świadczący usługę inicjowania płatności nie używają, nie uzyskują ani nie przechowują żadnych danych do celów innych niż do wykonania usługi inicjowania płatności wyraźnie zleconej przez płatnika. Ponadto w art. 67 ust. 2 lit. d) PSD2 ograniczono dostęp dostawcy świadczącego usługę dostępu do informacji o rachunku do informacji dotyczących wyznaczonych rachunków płatniczych i związanych z nimi transakcji płatniczych, podczas gdy art. 67 ust. 2 lit. f) tej dyrektywy stanowi, że dostawcy świadczący usługę dostępu do informacji o rachunku nie używają, nie uzyskują ani nie przechowują żadnych danych do celów innych niż do wykonania usługi dostępu do informacji o rachunku wyraźnie zleconej przez użytkownika usług płatniczych, zgodnie z przepisami o ochronie danych. W przepisach tych podkreślono, że w kontekście usług dostępu do informacji o rachunku dane osobowe można gromadzić wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach. Dostawca świadczący usługę dostępu do informacji o rachunku powinien zatem wyraźnie określić w umowie, do jakich konkretnych celów będą przetwarzane dane osobowe dotyczące informacji o rachunku w kontekście świadczonej przez niego usługi dostępu do informacji o rachunku. Umowa powinna być zgodna z prawem, rzetelna i przejrzysta, jak określono w art. 5 RODO, a także zgodna z innymi przepisami dotyczącymi ochrony konsumentów.

12. W zależności od konkretnych okoliczności dostawcy usług płatniczych mogą być administratorami lub podmiotami przetwarzającymi na podstawie RODO. W niniejszych wytycznych „administratorami" są ci dostawcy usług płatniczych, którzy samodzielnie lub wspólnie z innymi określają cele i sposoby przetwarzania danych osobowych. Więcej wskazówek na ten temat można znaleźć w Wytycznych EROD 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO.

2 ZGODNE Z PRAWEM PODSTAWY I DALSZE PRZETWARZANIE NA PODSTAWIE PSD2

2.1 Zgodne z prawem podstawy przetwarzania

13. Zgodnie z RODO administratorzy muszą mieć podstawę prawną, aby przetwarzać dane osobowe. Art. 6 ust. 1 RODO zawiera wyczerpujący i restrykcyjny wykaz sześciu podstaw prawnych przetwarzania danych osobowych zgodnie z RODO[13]. To do administratora należy określenie odpowiedniej podstawy prawnej i zapewnienie spełnienia wszystkich warunków dla tej podstawy prawnej. Określenie, która podstawa jest ważna i najodpowiedniejsza w konkretnej sytuacji, zależy od okoliczności, w jakich odbywa się przetwarzanie, w tym od celu przetwarzania i relacji między administratorem a osobą, której dane dotyczą.

2.2 Art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy)

14. Usługi płatnicze świadczy się na podstawie umowy pomiędzy użytkownikiem usług płatniczych a dostawcą usług płatniczych. Jak stwierdzono w motywie 87 PSD2, dyrektywa ta „powinna dotyczyć jedynie umownych zobowiązań i podziału odpowiedzialności między użytkownikiem usług płatniczych a dostawcą usług płatniczych.” Zgodnie z RODO główną podstawą prawną przetwarzania danych osobowych w celu świadczenia usług płatniczych jest art. 6 ust. 1 lit. b) RODO, a więc to, że przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

15. Usługi płatnicze w ramach PSD2 zdefiniowano w załączniku I do tej dyrektywy. Świadczenie tych usług w rozumieniu PSD2 jest wymogiem zawarcia umowy, w której strony mają dostęp do danych o rachunku płatniczym użytkownika usług płatniczych. Ponadto wspomniani dostawcy usług płatniczych muszą być licencjonowanymi operatorami. W odniesieniu do usług inicjowania płatności i usług dostępu do informacji o rachunku, o których mowa w PSD2, umowy mogą zawierać warunki służące nałożeniu również warunków dotyczących usług dodatkowych, których nie uregulowano w tej dyrektywie. W *Wytycznych EROD 2/2019 w sprawie przetwarzania danych*

[13] Zgodnie z art. 6 przetwarzanie danych osobowych jest zgodne z prawem, o ile ma zastosowanie co najmniej jeden z poniższych elementów:

(a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

(b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

(c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

(d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

(e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

(f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, wyjaśniono, że administratorzy muszą ocenić, jakie przetwarzanie danych osobowych jest obiektywnie niezbędne do wykonania umowy. W wytycznych tych wskazano, że uzasadnienie niezbędności zależy od charakteru usługi, wzajemnych interesów i oczekiwań stron umowy, uzasadnienia zawarcia umowy oraz istotnych elementów umowy.

16. W wytycznych EROD 2/2019 wyjaśniono również, że w świetle art. 7 ust. 4 RODO wprowadza się rozróżnienie pomiędzy czynnościami przetwarzania danych niezbędnymi do wykonania umowy a klauzulami uzależniającymi świadczenie usługi od dokonania pewnych czynności przetwarzania, które w rzeczywistości nie są niezbędne do wykonania umowy. „Niezbędne do wykonania" wyraźnie świadczy o tym, że wymaga się czegoś więcej niż tylko klauzuli umownej[14]. Administrator powinien być w stanie wykazać, w jaki sposób główny przedmiot konkretnej umowy zawartej z osobą, której dane dotyczą, nie będzie mógł zostać faktycznie realizowany bez przetwarzania danych osobowych. Samo odniesienie do przetwarzania danych lub wspomnienie o przetwarzaniu danych w umowie nie jest wystarczające, aby takie przetwarzanie objąć zakresem stosowania art. 6 ust. 1 lit. b) RODO.

17. W art. 5 ust. 1 lit. b) RODO przewidziano zasadę ograniczenia celu, zgodnie z którą wymaga się, aby dane osobowe były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Oceniając, czy art. 6 ust. 1 lit. b) stanowi właściwą podstawę prawną w kontekście usługi (płatniczej) online, należy uwzględnić szczególne zamierzenie, cel lub przeznaczenie tej usługi[15]. Cele przetwarzania należy jasno określić i powiadomić o nich osobę, której dane dotyczą, zgodnie z obowiązkami administratora w zakresie ograniczenia celu i przejrzystości. Ocena tego, co jest „niezbędne" obejmuje połączoną, opartą na faktach ocenę przetwarzania „w odniesieniu do zamierzonego celu oraz tego, czy przetwarzanie jest mniej inwazyjne w porównaniu z innymi metodami osiągnięcia tego samego celu". Art. 6 ust. 1 lit. b) nie obejmuje przetwarzania, które jest przydatne, ale nie jest obiektywnie niezbędne do wykonania usługi objętej umową lub podjęcia odpowiednich działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, nawet jeżeli jest ono niezbędne do innych celów biznesowych administratora[16].

18. W wytycznych EROD 2/2019 wyjaśniono, że w umowie nie można w sposób sztuczny rozszerzać kategorii danych osobowych ani rodzajów operacji przetwarzania, które administrator musi wykonać w celu wykonania umowy w rozumieniu art. 6 ust. 1 lit. b)[17]. Nawiązano w nich również do przypadków, w których może powstawać konieczność zaakceptowania całości umowy bądź jej odrzucenia przez osoby, których dane dotyczą, które mogą być zainteresowane tylko jedną z usług. Może to mieć miejsce, jeżeli administrator zechce połączyć kilka odrębnych usług lub elementów usługi o różnych podstawowych celach, cechach lub przesłankach w ramach jednej umowy. W przypadku gdy umowa obejmuje kilka odrębnych usług lub elementów usługi, które w rzeczywistości można wykonywać niezależnie od siebie, zastosowanie art. 6 ust. 1 lit. b) należy ocenić oddzielnie w kontekście każdej z tych usług, uwzględniając to, co jest obiektywnie

[14] Wytyczne EROD 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, s. 8.
[15] Tamże.
[16] Tamże, s. 7.
[17] Tamże, s. 10.

niezbędne do wykonania każdej z poszczególnych usług, których aktywnie zażądała osoba, której dane dotyczą, lub w odniesieniu do których dokonała rejestracji, by z nich korzystać[18].

19. Zgodnie z przytoczonymi wytycznymi administratorzy muszą ocenić, co jest obiektywnie niezbędne do wykonania umowy. Jeżeli administratorzy nie mogą wykazać, że przetwarzanie danych osobowych dotyczących rachunku płatniczego jest obiektywnie niezbędne do świadczenia każdej z tych usług z osobna, art. 6 ust. 1 lit. b) RODO nie stanowi ważnej podstawy prawnej przetwarzania. W takich przypadkach administrator powinien wziąć pod uwagę inną podstawę prawną przetwarzania.

2.3 Zapobieganie nadużyciom

20. Art. 94 ust. 1 PSD2 stanowi, że państwa członkowskie zezwalają na przetwarzanie danych osobowych przez systemy płatności i dostawców usług płatniczych, jeżeli jest to niezbędne, aby zagwarantować zapobieganie oszustwom płatniczym, prowadzenie dochodzeń w ich sprawie i wykrywanie ich. Prawnie uzasadnionym interesem dostawcy usług płatniczych, którego sprawa dotyczy, może być przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom, o ile charakteru nadrzędnego nie mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą[19]. Czynności przetwarzania w celu zapobiegania nadużyciom powinny opierać się na starannej ocenie poszczególnych przypadków przez administratora zgodnie z zasadą rozliczalności. Ponadto, aby zapobiec nadużyciom, administratorzy mogą również podlegać szczególnym zobowiązaniom prawnym, które wymagają przetwarzania danych osobowych.

2.4 Dalsze przetwarzanie (dostawcy świadczący usługę dostępu do informacji o rachunku i dostawcy świadczący usługę inicjowania płatności)

21. W art. 6 ust. 4 RODO określono warunki przetwarzania danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane. Dokładniej rzecz ujmując, takie dalsze przetwarzanie może się odbywać, jeśli opiera się na prawie Unii lub prawie państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, w przypadku gdy osoba, której dane dotyczą, wyraziła zgodę lub gdy przetwarzanie w celu innym niż cel, w którym zebrano dane osobowe, jest zgodne z pierwotnym celem.

22. Należy starannie uwzględnić art. 66 ust. 3 lit. g) i art. 67 ust. 2 lit. f) PSD2. Jak wspomniano powyżej, art. 66 ust. 3 lit. g) PSD2 stanowi, że dostawca świadczący usługę inicjowania płatności nie używa, nie uzyskuje ani nie przechowuje żadnych danych do celów innych niż do wykonania usługi inicjowania płatności wyraźnie zleconej przez płatnika. Art. 67 ust. 2 lit. f) PSD2 stanowi, że dostawca świadczący usługę dostępu do informacji o rachunku nie używa, nie uzyskuje ani nie przechowuje żadnych danych do celów innych niż do wykonania usługi dostępu do informacji o rachunku wyraźnie zleconej przez użytkownika usług płatniczych, zgodnie z przepisami o ochronie danych.

23. W związku z tym art. 66 ust. 3 lit. g) i art. 67 ust. 2 lit. f) PSD2 znacznie ograniczają możliwości przetwarzania w innym celu, co oznacza, że przetwarzanie w innym celu jest niedozwolone, chyba że osoba, której dane dotyczą, wyraziła zgodę zgodnie z art. 6 ust. 1 lit. a) RODO lub przetwarzanie przewidziano w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator, zgodnie z art. 6 ust. 4 RODO. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub

[18] Tamże, s. 11.
[19] Motyw 47 RODO.

prawa państwa członkowskiego, ograniczenia określone w art. 66 ust. 3 lit. g) i art. 67 ust. 2 lit. f) PSD2 wyraźnie wskazują, że jakikolwiek inny cel nie jest zgodny z celem, w którym dane osobowe zostały pierwotnie zebrane. W oparciu o test zgodności, o którym mowa w art. 6 ust. 4 RODO, nie można stwierdzić podstawy prawnej przetwarzania danych.

24. Art. 6 ust. 4 RODO umożliwia dalsze przetwarzanie na podstawie prawa Unii lub prawa państwa członkowskiego. Na przykład wszyscy dostawcy świadczący usługę inicjowania płatności i dostawcy świadczący usługę dostępu do informacji o rachunku są podmiotami zobowiązanymi zgodnie z art. 3 pkt 2 lit. a) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy). Te podmioty zobowiązane są zatem zmuszone do stosowania środków należytej staranności wobec klienta określonych w dyrektywie. Dane osobowe przetwarzane w związku z usługą objętą zakresem PSD2 są w związku z tym przetwarzane dalej na podstawie co najmniej jednego zobowiązania prawnego spoczywającego na dostawcy usług[20].

25. Jak wspomniano w pkt 20, z art. 6 ust. 4 RODO wynika, że przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, może opierać się na zgodzie osoby, której dane dotyczą, jeśli spełniono wszystkie warunki wyrażenia zgody określone w RODO. Jak określono powyżej, administrator musi wykazać, że istnieje możliwość odmowy lub wycofania zgody bez niekorzystnych konsekwencji (motyw 42 RODO).

2.5 Zgodna z prawem podstawa udzielenia dostępu do rachunku (dostawcy usług płatniczych prowadzący rachunek)

26. Jak wspomniano w pkt 10, użytkownicy usług płatniczych mogą realizować prawo do korzystania z usług inicjowania płatności i usług dostępu do informacji o rachunku. Obowiązki nałożone na państwa członkowskie w art. 66 ust. 1 i art. 67 ust. 1 PSD2 należy wdrożyć do prawa krajowego w celu zagwarantowania skutecznego stosowania prawa użytkownika usług płatniczych do korzystania z wyżej wymienionych usług płatniczych. Skuteczne stosowanie takich praw nie byłoby możliwe bez istnienia spoczywającego na dostawcy usług płatniczych prowadzącym rachunek, zazwyczaj banku, powiązanego obowiązku udzielenia dostawcy usług płatniczych dostępu do rachunku, pod warunkiem że spełnił on wszystkie wymogi niezbędne do uzyskania dostępu do rachunku użytkownika usług płatniczych. Ponadto art. 66 ust. 5 i art. 67 ust. 4 PSD2 stanowią wyraźnie, że świadczenia usług inicjowania płatności oraz usług dostępu do informacji o rachunku nie można uzależniać od istnienia stosunku umownego pomiędzy dostawcą świadczącym usługę inicjowania płatności/dostawcą świadczącym usługę dostępu do informacji o rachunku a dostawcą usług płatniczych prowadzącym rachunek.

27. Przetwarzanie danych osobowych przez dostawcę usług płatniczych prowadzącego rachunek polegające na udostępnieniu danych osobowych na żądanie dostawcy świadczącego usługę inicjowania płatności i dostawcy świadczącego usługę dostępu do informacji o rachunku w celu świadczenia przez nich usługi płatniczej na rzecz użytkownika usług płatniczych wynika z obowiązku prawnego. Aby osiągnąć cele określone w PSD2, dostawcy usług płatniczych prowadzący rachunek muszą dostarczać dane osobowe na potrzeby usług świadczonych przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku, co jest warunkiem koniecznym do świadczenia usług przez tych

[20] Należy zauważyć, że dokładna analiza tego, czy dyrektywa w sprawie przeciwdziałania praniu pieniędzy odpowiada normie określonej w art. 6 ust. 4 RODO, wykracza poza zakres niniejszego dokumentu.

dostawców, a tym samym zapewnienia praw przewidzianych w art. 66 ust. 1 i art. 67 ust. 1 PSD2. W związku z tym właściwą podstawą prawną w tym przypadku jest art. 6 ust. 1 lit. c) RODO.

28. Ponieważ w RODO określono, że przetwarzanie na podstawie obowiązku prawnego powinno być wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego (zob. art. 6 ust. 3 RODO), obowiązek udzielenia dostępu przez dostawców usług płatniczych prowadzących rachunek powinien wynikać z prawa krajowego transponującego PSD2.

3 WYRAŹNA ZGODA

3.1 Zgoda w rozumieniu RODO

29. Zgodnie z RODO zgoda stanowi jedną z sześciu podstaw prawnych zgodności przetwarzania danych osobowych z prawem. Art. 4 ust. 11 RODO definiuje zgodę jako „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych". Te cztery warunki, „dobrowolne, konkretne, świadome i jednoznaczne", są niezbędne dla ważności zgody. Zgodnie ze sporządzonymi przez EROD Wytycznymi 05/2020 dotyczącymi zgody na mocy rozporządzenia 2016/679 zgoda może być właściwą, zgodną z prawem podstawą wyłącznie wówczas, gdy osobie, której dane dotyczą, zapewnia się kontrolę oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia zaoferowanych warunków lub odrzucenia ich bez niekorzystnych konsekwencji. Zwracając się o zgodę, administrator ma obowiązek oceny, czy spełni wszystkie wymogi uzyskania ważnej zgody. Zgoda uzyskana w pełnej zgodności z RODO jest narzędziem zapewniającym osobom, których dane dotyczą, kontrolę nad tym, czy dotyczące ich dane osobowe będą przetwarzane. W braku zgodności zgody z RODO kontrola ze strony osoby, której dane dotyczą, staje się złudna, a zgoda będzie nieważną podstawą prawną przetwarzania, co spowoduje niezgodność z prawem czynności przetwarzania[21].

30. RODO zawiera również dalsze zabezpieczenia opisane w art. 7, który stanowi, że administrator musi być w stanie wykazać, że w chwili przetwarzania danych dysponował ważną zgodą. Ponadto zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Oprócz tego osoba, której dane dotyczą, musi zostać poinformowana o prawie do wycofania zgody w dowolnym momencie, przy czym takie wycofanie zgody musi być równie łatwe jak jej wyrażenie.

31. Zgodnie z art. 9 RODO zgoda jest jednym z wyjątków od ogólnego zakazu przetwarzania szczególnych kategorii danych osobowych. W takim przypadku zgoda osoby, której dane dotyczą, musi być jednak „wyraźna"[22].

32. Zgodnie ze sporządzonymi przez EROD Wytycznymi 05/2020 dotyczącymi zgody na mocy rozporządzenia 2016/679 wyraźna zgoda, o której mowa w RODO, odnosi się do sposobu wyrażenia zgody przez osobę, której dane dotyczą. Oznacza to, że osoba, której dane dotyczą, powinna złożyć w sposób wyraźny oświadczenie o wyrażeniu zgody na określony cel lub określone cele przetwarzania. Oczywistym sposobem zapewnienia, aby zgoda była wyraźna, byłoby jej wyraźne potwierdzenie w pisemnym oświadczeniu. W stosownych przypadkach administrator mógłby zapewnić podpisanie pisemnego oświadczenia przez osobę, której dane dotyczą, aby rozwiać wszelkie możliwe wątpliwości i zapobiec możliwemu brakowi dowodów w przyszłości.

33. W żadnym wypadku zgoda nie może być wywnioskowana z potencjalnie niejednoznacznych oświadczeń lub działań. Administrator musi również mieć świadomość, że zgody nie można uzyskać w drodze tej samej czynności co zawarcie umowy czy zaakceptowanie ogólnych warunków usługi.

3.2 Zgoda w rozumieniu PSD2

[21] EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, pkt 3.

[22] Zob. także opinia 15/2011 w sprawie definicji zgody (WP 187), s. 6–8, lub opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP 217), s. 9, 10, 13 i 14.

34. EROD zauważa, że ramy prawne dotyczące wyraźnej zgody są skomplikowane, ponieważ pojęcie „wyraźnej zgody" znajduje się zarówno w PSD2, jak i w RODO. Nasuwa się pytanie, czy „wyraźną zgodę", o której mowa w art. 94 ust. 2 PSD2, należy interpretować w taki sam sposób jak wyraźną zgodę na mocy RODO.

3.2.1 Wyraźna zgoda w rozumieniu art. 94 ust. 2 PSD2

35. PSD2 zawiera szereg szczegółowych zasad dotyczących przetwarzania danych osobowych, w szczególności w art. 94 ust. 1, który stanowi, że przetwarzanie danych osobowych na potrzeby PSD2 musi odbywać się zgodnie z unijnymi przepisami o ochronie danych. Ponadto art. 94 ust. 2 PSD2 stanowi, że dostawcy usług płatniczych uzyskują dostęp jedynie do danych osobowych niezbędnych do świadczenia swoich usług płatniczych, przetwarzają te dane i zatrzymują je za wyraźną zgodą użytkownika usług płatniczych. Zgodnie z art. 33 ust. 2 PSD2 wymóg wyraźnej zgody użytkownika usług płatniczych nie ma zastosowania do dostawców świadczących usługę dostępu do informacji o rachunku. W art. 67 ust. 2 lit. a) PSD2 przewiduje się jednak konieczność uzyskania wyraźnej zgody na świadczenie usługi przez dostawców świadczących usługę dostępu do informacji o rachunku.

36. Jak wspomniano powyżej, lista zgodnych z prawem podstaw przetwarzania na podstawie RODO jest wyczerpująca. Jak wspomniano w pkt 14, podstawą prawną przetwarzania danych osobowych w celu świadczenia usług płatniczych jest zasadniczo art. 6 ust. 1 lit. b) RODO, a więc to, że przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Wynika z tego, że art. 94 ust. 2 PSD2 nie można uznać za dodatkową podstawę prawną przetwarzania danych osobowych. EROD uważa, że w związku z powyższym ustęp ten należy interpretować z jednej strony zgodnie z mającymi zastosowanie ramami prawnymi ochrony danych, a z drugiej strony w sposób zachowujący jego skuteczność. Wyraźną zgodę w rozumieniu art. 94 ust. 2 PSD2 należy zatem uznać za dodatkowy wymóg o charakterze umownym[23] w odniesieniu do dostępu do danych osobowych, a następnie ich przetwarzania i przechowywania na potrzeby świadczenia usług płatniczych, a zatem taka zgoda nie jest tożsama z (wyraźną) zgodą na podstawie RODO.

37. „Wyraźna zgoda", o której mowa w art. 94 ust. 2 PSD2, jest zgodą umowną. Oznacza to, że art. 94 ust. 2 PSD2 należy interpretować w ten sposób, że zawierając umowę z dostawcą usług płatniczych na podstawie tej dyrektywy, osoby, których dane dotyczą, muszą być w pełni świadome szczególnych kategorii danych osobowych, które będą przetwarzane. Ponadto należy poinformować je o konkretnym celu (usługa płatnicza), w którym ich dane osobowe będą przetwarzane, i muszą one wyraźnie zgodzić się na te klauzule. Klauzule takie powinny wyraźnie odróżniać się od pozostałych kwestii poruszanych w umowie, a osoba, której dane dotyczą, musiałaby wyraźnie je zaakceptować.

38. Kluczowym elementem w kontekście pojęcia „wyraźnej zgody" w rozumieniu art. 94 ust. 2 PSD2 jest uzyskanie dostępu do danych osobowych w celu późniejszego przetwarzania i przechowywania tych danych na potrzeby świadczenia usług płatniczych. Oznacza to, że dostawca usług płatniczych[24] nie przetwarza jeszcze danych osobowych, ale potrzebuje dostępu do danych osobowych, które przetwarzano na odpowiedzialność innego administratora. Jeśli użytkownik usług płatniczych zawiera umowę na przykład z dostawcą świadczącym usługę inicjowania płatności, dostawca ten musi uzyskać dostęp do danych osobowych użytkownika usług płatniczych, za których przetwarzanie odpowiedzialny jest dostawca usług płatniczych prowadzący rachunek.

[23] Pismo EROD w sprawie drugiej dyrektywy w sprawie usług płatniczych, 5 lipca 2018 r., s. 4.
[24] Dotyczy to usług 1–7 wymienionych w załączniku I do PSD2.

Przedmiotem wyraźnej zgody, o której mowa w art. 94 ust. 2 PSD2, jest zezwolenie na uzyskanie dostępu do tych danych osobowych w celu umożliwienia przetwarzania i przechowywania tych danych osobowych, które są niezbędne w celu świadczenia usługi płatniczej. W przypadku wyrażenia wyraźnej zgody przez osobę, której dane dotyczą, dostawca usług płatniczych prowadzący rachunek zobowiązany jest do udzielenia dostępu do wskazanych danych osobowych.

39. Mimo że zgoda, o której mowa w art. 94 ust. 2 PSD2, nie stanowi podstawy prawnej przetwarzania danych osobowych, jest ona szczególnie związana z danymi osobowymi i ochroną danych oraz zapewnia przejrzystość i pewien stopień kontroli dla użytkownika usług płatniczych[25]. Chociaż w PSD2 nie określono materialnych przesłanek zgody, o której mowa w art. 94 ust. 2 tej dyrektywy, należy ją, jak stwierdzono powyżej, rozumieć zgodnie z mającymi zastosowanie ramami prawnymi ochrony danych oraz w sposób pozwalający zachować jej skuteczność.

40. W odniesieniu do informacji, które mają być dostarczane przez administratorów, i wymogu przejrzystości w Wytycznych Grupy Roboczej Art. 29 w sprawie przejrzystości stwierdzono, że „[n]ajważniejszym aspektem zasady przejrzystości, którą określono we wspomnianych przepisach, jest to, że osoba, której dane dotyczą, powinna zawsze być w stanie z wyprzedzeniem określić zakres i skutki przetwarzania i że nie powinna zostać później zaskoczona informacją, w jaki sposób wykorzystano jej dane osobowe”[26].

41. Ponadto zgodnie z zasadą ograniczenia celu dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach (art. 5 ust. 1 lit. b) RODO). Jeśli dane osobowe gromadzi się w więcej niż jednym celu, „administratorzy powinni unikać określania wyłącznie jednego ogólnego celu, aby uzasadnić różne czynności dalszego przetwarzania, które w rzeczywistości są tylko w niewielkim stopniu związane z rzeczywistym pierwotnym celem”[27]. EROD podkreśliła, ostatnio w kontekście umów dotyczących usług online, ryzyko związane z zawieraniem w umowach warunków ogólnych przetwarzania i stwierdziła, że cel zbierania danych musi być jasno i konkretnie określony: powinien być wystarczająco szczegółowy, aby określić, jaki rodzaj przetwarzania danych jest objęty określonym celem, a jaki nie jest, oraz aby umożliwić ocenę zgodności z prawem i zastosowanie zabezpieczeń ochrony danych[28].

42. W kontekście dodatkowego wymogu dotyczącego wyraźnej zgody zgodnie z art. 94 ust. 2 PSD2 oznacza to, że administratorzy muszą udzielić osobom, których dane dotyczą, konkretnych i wyraźnych informacji o określonych przez administratora konkretnych celach, w których ich dane osobowe są udostępniane, przetwarzane i zatrzymywane. Zgodnie z art. 94 ust. 2 PSD2, osoby, których dane dotyczą, muszą wyraźnie zaakceptować te konkretne cele.

43. Ponadto, jak wskazano w pkt 10 powyżej, EROD podkreśla, że użytkownik usług płatniczych musi mieć możliwość wyboru, czy chce korzystać z danej usługi czy nie, i nie może być do tego zmuszany. Zgoda, o której mowa w art. 94 ust. 2 PSD2, musi być również zgodą wyrażoną dobrowolnie.

3.3 Podsumowanie

[25] Art. 94 ust. 2 PSD2 wchodzi w zakres rozdziału 4 „Ochrona danych”.
[26] Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, pkt 10 (przyjęte w dniu 11 kwietnia 2018 r.) – zatwierdzone przez EROD.
[27] Opinia Grupy Roboczej Art. 29 03/2013 w sprawie ograniczenia celu (WP203), s. 16.
[28] Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, pkt 16 (wersja do konsultacji publicznych) oraz opinia 03/2013 Grupy Roboczej Art. 29 w sprawie ograniczenia celu (WP203), s. 15–16.

44. Wyraźna zgoda w rozumieniu PSD2 różni się od (wyraźnej) zgody w rozumieniu RODO. Wyraźna zgoda na podstawie art. 94 ust. 2 PSD2 jest dodatkowym wymogiem o charakterze umownym. Jeśli dostawca usług płatniczych potrzebuje dostępu do danych osobowych w celu świadczenia usługi płatniczej, zgodnie z art. 94 ust. 2 PSD2 konieczna jest wyraźna zgoda użytkownika usług płatniczych.

4 PRZETWARZANIE DANYCH MILCZĄCEJ STRONY

4.1 Dane milczącej strony

45. Kwestią związaną z ochroną danych, która wymaga starannego uwzględnienia, jest przetwarzanie tak zwanych danych milczącej strony. W kontekście niniejszego dokumentu dane milczącej strony to dane osobowe osoby, której dane dotyczą, która nie jest użytkownikiem określonego dostawcy usług płatniczych, ale której dane osobowe są przetwarzane przez tego określonego dostawcę usług płatniczych w celu wykonania umowy między dostawcą a użytkownikiem usług płatniczych. Dzieje się tak na przykład w przypadku, gdy użytkownik usług płatniczych, osoba A, której dane dotyczą, korzysta z usług dostawcy świadczącego usługę dostępu do informacji o rachunku, a osoba B, której dane dotyczą, dokonała serii transakcji płatniczych na rachunek płatniczy osoby A, której dane dotyczą. W tym przypadku osobę B, której dane dotyczą, uważa się za „milczącą stronę", a dane osobowe (takie jak numer rachunku osoby B, której dane dotyczą, i kwota będąca przedmiotem tych transakcji) osoby B, której dane dotyczą, uważa się za „dane milczącej strony".

4.2 Prawnie uzasadniony interes administratora

46. W art. 5 ust. 1 lit. b) RODO zawarto wymóg, aby dane osobowe były wyłącznie zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i aby nie można było przetwarzać ich dalej w sposób niezgodny z tymi celami. Ponadto w RODO wymaga się, aby wszelkie przetwarzanie danych osobowych było zarówno niezbędne, jak i proporcjonalne oraz zgodne z zasadami ochrony danych, takimi jak zasada ograniczenia celu i zasada minimalizacji danych.

47. Przetwarzanie danych milczącej strony na podstawie RODO jest możliwe, gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (art. 6 ust. 1 lit. f) RODO). Takie przetwarzanie może mieć jednak miejsce jedynie wówczas, gdy wobec prawnie uzasadnionego interesu realizowanego przez administratora „nadrzędnego charakteru nie mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych".

48. Podstawą prawną przetwarzania danych milczącej strony przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku – w kontekście świadczenia usług płatniczych na podstawie PSD2 – może być zatem prawnie uzasadniony interes administratora lub strony trzeciej, polegający na wykonaniu umowy z użytkownikiem usług płatniczych. Konieczność przetwarzania danych osobowych milczącej strony jest ograniczona i ustalana na podstawie rozsądnych oczekiwań tych osób, których dane dotyczą. W kontekście świadczenia usług płatniczych objętych PSD2 należy ustanowić skuteczne i odpowiednie środki w celu zagwarantowania, że interesy lub podstawowe prawa i wolności milczących stron będą miały nadrzędny charakter, oraz w celu zapewnienia poszanowania rozsądnych oczekiwań osób, których dane dotyczą, w odniesieniu do przetwarzania ich danych osobowych. W tym względzie administrator (dostawca świadczący usługę dostępu do informacji o rachunku lub dostawca świadczący usługę inicjowania płatności) musi ustanowić niezbędne zabezpieczenia w zakresie przetwarzania danych w celu ochrony praw osób, których dane dotyczą. Obejmuje to środki techniczne zapewniające, aby danych milczącej strony nie przetwarzano w celu innym niż cel, w którym dane osobowe zostały pierwotnie zebrane przez dostawców świadczących usługę inicjowania płatności i dostawców świadczących usługę dostępu do informacji o rachunku. Jeśli jest to wykonalne, należy również zastosować szyfrowanie lub inne techniki w celu osiągnięcia odpowiedniego poziomu bezpieczeństwa i minimalizacji danych.

4.3 Dalsze przetwarzanie danych osobowych milczącej strony

49. Jak stwierdzono w pkt 29, dane osobowe przetwarzane w związku z usługą płatniczą uregulowaną w PSD2 mogłyby być przetwarzane dalej na podstawie zobowiązań prawnych spoczywających na dostawcy usług. Wspomniane zobowiązania prawne mogłyby dotyczyć danych osobowych milczącej strony.

50. W odniesieniu do dalszego przetwarzania danych milczącej strony na podstawie prawnie uzasadnionego interesu EROD jest zdania, że dane te nie mogą być wykorzystywane w celu innym niż cel, w którym dane osobowe zostały zebrane, chyba że odbywa się to na podstawie prawa Unii lub państwa członkowskiego. Uzyskanie zgody milczącej strony jest niewykonalne z prawnego punktu widzenia, ponieważ w celu uzyskania takiej zgody konieczne byłoby zbieranie lub przetwarzanie danych osobowych milczącej strony, dla których to działań nie można znaleźć podstawy prawnej w art. 6 RODO. W oparciu o test zgodności, o którym mowa w art. 6 ust. 4 RODO, również nie można stwierdzić podstawy przetwarzania danych do innych celów (np. działań z zakresu marketingu bezpośredniego). Prawa i wolności tych milczących stron będących osobami, których dane dotyczą, nie będą przestrzegane, jeżeli nowy administrator wykorzysta dane osobowe do innych celów, biorąc pod uwagę kontekst, w jakim zebrano dane osobowe, w szczególności: brak jakiegokolwiek związku z osobami, których dane dotyczą, będącymi milczącymi stronami[29]; brak związku pomiędzy jakimkolwiek innym celem a celem, w którym dane osobowe zostały pierwotnie zebrane (tj. fakt, że dostawcy usług płatniczych potrzebują danych milczącej strony wyłącznie w celu wykonania umowy z drugą umawiającą się stroną); charakter przedmiotowych danych osobowych[30], okoliczność, że osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania, lub nawet mogą nie być świadome, który administrator może przetwarzać ich dane osobowe, oraz biorąc pod uwagę ograniczenia prawne dotyczące przetwarzania określone w art. 66 ust. 3 lit. g) i w art. 67 ust. 2 lit. f) PSD2.

[29] Motyw 87 PSD2 stanowi, że dyrektywa ta dotyczy jedynie „umownych zobowiązań i podziału odpowiedzialności między użytkownikiem usług płatniczych a dostawcą usług płatniczych". Dane milczącej strony nie są zatem objęte zakresem PSD2.

[30] Należy zachować szczególną ostrożność przy przetwarzaniu finansowych danych osobowych, ponieważ zgodnie z wytycznymi dotyczącymi oceny skutków dla ochrony danych przetwarzanie to można uznać za zwiększające możliwe ryzyko naruszenia praw i wolności osób.

5 PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH NA PODSTAWIE PSD2

5.1 Szczególne kategorie danych osobowych

51. Zgodnie z art. 9 ust. 1 RODO zabrania się „przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby".

52. Należy podkreślić, że w niektórych państwach członkowskich płatności elektroniczne są już powszechne i wiele osób preferuje je zamiast gotówki w codziennych transakcjach. Jednocześnie transakcje finansowe mogą ujawniać informacje szczególnie chronione o konkretnej osobie, której danej dotyczą, w tym informacje dotyczące szczególnych kategorii danych osobowych. Na przykład, w zależności od szczegółów transakcji, na podstawie darowizn przekazywanych na rzecz partii lub organizacji politycznych, kościołów lub parafii mogą zostać ujawnione poglądy polityczne i przekonania religijne. Na podstawie potrącania rocznej składki członkowskiej z rachunku bankowego danej osoby może zostać ujawnione jej członkostwo w związku zawodowym. Na podstawie analizy rachunków opłacanych przez osobę, której dane dotyczą, na rzecz lekarza (np. psychiatry) mogą być zbierane dane osobowe dotyczące zdrowia. Ponadto informacje dotyczące określonych zakupów mogą ujawniać informacje o seksualności osoby lub jej orientacji seksualnej. Jak wynika z tych przykładów, każda transakcja może zawierać szczególne kategorie danych osobowych. Ponadto usługi dostępu do informacji o rachunku mogą opierać się na profilowaniu zdefiniowanym w art. 4 pkt 4 RODO. Jak stwierdzono uprzednio w sporządzonych przez Grupę Roboczą Art. 29 i zatwierdzonych przez EROD Wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, „[p]rofilowanie może doprowadzić do stworzenia danych szczególnej kategorii wskutek ich wywnioskowania z danych, które same w sobie nie są danymi szczególnej kategorii, ale które stają się nimi w momencie ich połączenia z innymi danymi"[31]. Oznacza to, że na podstawie sumy transakcji finansowych mogą zostać ujawnione różne wzorce zachowań, które mogą obejmować szczególne kategorie danych osobowych. Istnieje zatem duże prawdopodobieństwo, że dostawca usług przetwarzający informacje dotyczące transakcji finansowych osób, których dane dotyczą, przetwarza również szczególne kategorie danych osobowych.

53. W odniesieniu do terminu „szczególnie chronione dane dotyczące płatności" EROD zauważa, co następuje. Definicja szczególnie chronionych danych dotyczących płatności zawarta w PSD2 różni się znacząco od sposobu, w jaki termin „dane wrażliwe" jest powszechnie stosowany w kontekście RODO i (przepisów dotyczących) ochrony danych. Podczas gdy w PSD2 „szczególnie chronione dane dotyczące płatności" zdefiniowano jako „dane, w tym indywidualne dane uwierzytelniające, które mogą być wykorzystywane do dokonywania oszustw", w RODO podkreśla się potrzebę szczególnej ochrony szczególnych kategorii danych osobowych, które – zgodnie z art. 9 RODO – z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności[32]. W związku z tym zaleca się co najmniej określenie, jakiego rodzaju dane osobowe będą

[31] Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, WP251rev.01, s. 15.

[32] Na przykład w motywie 10 RODO szczególne kategorie danych osobowych określa się jako „dane wrażliwe".

przetwarzane, oraz wskazanie kategorii tych danych. Najprawdopodobniej konieczne będzie przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 RODO, która pomoże w takiej identyfikacji. Więcej wytycznych dotyczących oceny skutków dla ochrony danych można znaleźć w sporządzonych przez Grupę Roboczą Art. 29 Wytycznych dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, zatwierdzone przez EROD.

5.2 Możliwe wyjątki

54. Zakaz zawarty w art. 9 RODO nie jest bezwzględny. W szczególności, o ile wyjątki określone w art. 9 ust. 2 lit. b)–f) i h)–j) RODO wyraźnie nie mają zastosowania do przetwarzania danych osobowych w kontekście PSD2, można rozważyć dwa wyjątki przewidziane w art. 9 ust. 2 RODO:

a) Zakaz nie ma zastosowania w przypadku, gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach (art. 9 ust. 2 lit. a) RODO).

b) Zakaz nie ma zastosowania w przypadku, gdy przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. g) RODO).

55. Należy zauważyć, że wykaz wyjątków przewidzianych w art. 9 ust. 2 RODO jest wyczerpujący. Dostawca usług musi uznać możliwość włączenia szczególnych kategorii danych osobowych do danych osobowych przetwarzanych w celu świadczenia usług objętych zakresem PSD2. Ponieważ zakaz zawarty w art. 9 ust. 1 RODO ma zastosowanie do tych dostawców usług, muszą oni upewnić się, że w ich przypadku zastosowanie ma jeden z wyjątków przewidzianych w art. 9 ust. 2 RODO. Należy podkreślić, że w przypadku gdy usługodawca nie może wykazać, że spełniono warunki jednego z wyjątków, zakaz zawarty w art. 9 ust. 1 ma zastosowanie.

5.3 Ważny interes publiczny

56. Usługi płatnicze mogą obejmować przetwarzanie szczególnych kategorii danych osobowych ze względów związanych z ważnym interesem publicznym, ale jedynie w przypadku, gdy spełniono wszystkie warunki określone w art. 9 ust. 2 lit. g) RODO. Oznacza to, że przetwarzanie szczególnych kategorii danych osobowych musi zostać uregulowane w szczególnym wyjątku od art. 9 ust. 1 RODO w prawie Unii lub państwa członkowskiego. Przepis ten będzie musiał uwzględniać proporcjonalność w stosunku do zamierzonego celu przetwarzania oraz zawierać odpowiednie i konkretne środki ochrony praw podstawowych i interesów osób, których dane dotyczą. Ponadto taki przepis na mocy prawa Unii lub prawa państwa członkowskiego będzie musiał respektować istotę prawa do ochrony danych. Co więcej, należy również wykazać, że przetwarzanie szczególnych kategorii danych jest niezbędne ze względu na ważny interes publiczny, w tym interesy o znaczeniu systemowym. Dopiero gdy wszystkie te warunki zostaną w pełni spełnione, wyjątek ten będzie mógł mieć zastosowanie do określonych rodzajów usług płatniczych.

5.4 Wyraźna zgoda

57. W przypadkach, w których wyjątek przewidziany w art. 9 ust. 2 lit. g) RODO nie ma zastosowania, wydaje się, że uzyskanie wyraźnej zgody zgodnie z warunkami ważnej zgody określonymi w RODO pozostaje jedynym możliwym zgodnym z prawem wyjątkiem w odniesieniu do przetwarzania szczególnych kategorii danych osobowych przez dostawców usług będących osobami trzecimi. W

Wytycznych 05/2020 dotyczących zgody na mocy rozporządzenia 2016/679 EROD stwierdza się[33], że „[w] art. 9 ust. 2 nie przewidziano, by charakter danych »niezbędnych do wykonania umowy« był wyjątkiem od ogólnego zakazu przetwarzania szczególnych kategorii danych. W związku z tym administratorzy i państwa członkowskie, które znajdują się w takiej sytuacji, powinni zbadać konkretne wyjątki przewidziane w art. 9 ust. 2 lit. b)–j)". Jeżeli dostawcy usług opierają się na art. 9 ust. 2 lit. a) RODO, muszą upewnić się, że przed przystąpieniem do przetwarzania uzyskali wyraźną zgodę. Wyraźna zgoda, o której mowa w art. 9 ust. 2 lit. a) RODO, musi spełniać wszystkie wymogi RODO.

5.5 Brak odpowiedniego wyjątku

58. Jak zauważono powyżej, gdy usługodawca nie może wykazać, że spełniono warunki jednego z wyjątków, zakaz zawarty w art. 9 ust. 1 ma zastosowanie. W takim przypadku można wprowadzić środki techniczne, aby zapobiec przetwarzaniu szczególnych kategorii danych osobowych, na przykład poprzez uniemożliwienie przetwarzania niektórych punktów danych. W tym względzie dostawcy usług płatniczych mogą zbadać techniczne możliwości wyłączenia szczególnych kategorii danych osobowych i umożliwienia wybranego dostępu, co zapobiegłoby przetwarzaniu szczególnych kategorii danych osobowych dotyczących milczących stron przez dostawców usług będących osobami trzecimi.

[33] EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, pkt 99.

6 MINIMALIZACJA DANYCH, BEZPIECZEŃSTWO, PRZEJRZYSTOŚĆ, ROZLICZALNOŚĆ I PROFILOWANIE

6.1 Minimalizacja danych i uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

59. Zasada minimalizacji danych jest zapisana w art. 5 ust. 1 lit. c) RODO: „Dane osobowe muszą być […] adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane". Zasadniczo, zgodnie z zasadą minimalizacji danych, administratorzy nie powinni przetwarzać więcej danych osobowych niż jest to konieczne do osiągnięcia danego celu. Jak wskazano w rozdziale 2, ilość i rodzaj danych osobowych niezbędnych do świadczenia usługi płatniczej określa się na podstawie obiektywnego i wspólnie uzgodnionego celu umowy[34]. Minimalizacja danych ma zastosowanie przy każdym przetwarzaniu (np. przy każdym zbieraniu danych osobowych, dostępie do nich i ich żądaniu). W Wytycznych 4/2019 dotyczących artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrony danych z EROD stwierdza, że „podmioty przetwarzające i dostawców technologii również uznaje się za kluczowe podmioty umożliwiające uwzględnianie ochrony danych w fazie projektowania oraz domyślną ochronę danych; powinni oni również mieć świadomość, że administratorzy są zobowiązani do przetwarzania danych osobowych wyłącznie za pomocą systemów i technologii, które mają wbudowany mechanizm ochrony danych"[35].

60. Art. 25 RODO zawiera obowiązki uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych. Obowiązki te mają szczególne znaczenie dla zasady minimalizacji danych. Artykuł ten stanowi, że administratorzy – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdrażają odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Środki te mogą obejmować szyfrowanie, pseudonimizację i inne środki techniczne.

61. W przypadku stosowania obowiązku wynikającego z art. 25 RODO elementami, które należy uwzględnić, są stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, jakie stwarza przetwarzanie. Dalsze wyjaśnienia dotyczące tego obowiązku znajdują się we wspomnianych wyżej Wytycznych EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z art. 25.

6.2 Środki minimalizacji danych

62. Dostawca usług będący osobą trzecią uzyskujący dostęp do danych rachunku płatniczego w celu świadczenia żądanych usług musi również uwzględniać zasadę minimalizacji danych i musi gromadzić wyłącznie dane osobowe niezbędne do świadczenia konkretnych usług płatniczych,

[34] EROD, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, pkt 32.
[35] EROD, Wytyczne 4/2019 dotyczące artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych, s. 29.

o które zwrócił się użytkownik usług płatniczych. Co do zasady, dostęp do danych osobowych powinien być ograniczony do zakresu niezbędnego do świadczenia usług płatniczych. Jak wykazano w rozdziale 2, PSD2 nakłada na dostawców usług płatniczych prowadzących rachunek obowiązek udostępniania informacji o użytkowniku usług płatniczych na wniosek użytkownika usług płatniczych, gdy ten chce skorzystać z usługi inicjowania płatności lub usługi dostępu do informacji o rachunku.

63. W przypadku gdy nie wszystkie dane dotyczące rachunku płatniczego są niezbędne do wykonania umowy, dostawca świadczący usługę dostępu do informacji o rachunku powinien dokonać wyboru odpowiednich kategorii danych przed ich zgromadzeniem. Na przykład kategorie danych, które mogą nie być niezbędne, mogą obejmować tożsamość milczącej strony i charakterystykę transakcji. Ponadto, o ile nie wymaga tego prawo państwa członkowskiego lub prawo Unii, nie ma potrzeby podawania IBAN rachunku bankowego milczącej strony.

64. W tym względzie można rozważyć ewentualne zastosowanie środków technicznych, które umożliwiają dostawcom usług będących osobami trzecimi wypełnianie ich obowiązku dotyczącego dostępu do jedynie tych danych osobowych i pobierania jedynie tych danych osobowych, które są niezbędne do świadczenia ich usług, lub wspierają dostawców w wypełnianiu tego obowiązku, w ramach wdrażania odpowiednich polityk ochrony danych, zgodnie z art. 24 ust. 2 RODO. W tym względzie EROD zaleca stosowanie narzędzi cyfrowych w celu wspierania dostawców świadczących usługę dostępu do informacji o rachunku w wypełnianiu ich obowiązku gromadzenia wyłącznie tych danych osobowych, które są niezbędne do celów, do których są one przetwarzane. Na przykład, gdy dostawca usług nie potrzebuje charakterystyki transakcji (w polu opisu zapisów transakcji) do świadczenia swoich usług, cyfrowe narzędzie wyboru mogłoby funkcjonować jako środek umożliwiający dostawcom usług będącym osobami trzecimi wyłączenie tego pola z ogólnych operacji przetwarzania przez tych dostawców.

Przykład 2:

HappyPayments, nasz dostawca usług dostępu do informacji o rachunku z przykładu 1, chce zapewnić, aby w ramach jego usług przetwarzane były wyłącznie te dane osobowe dotyczące rachunku płatniczego, którymi są zainteresowani jego użytkownicy. Uzyskanie dostępu do większej ilości danych dotyczących rachunku płatniczego nie byłoby konieczne do świadczenia usługi. W związku z tym umożliwia użytkownikom wybór konkretnych rodzajów informacji, którymi są zainteresowani.

Użytkownik A chce mieć przegląd swoich wydatków z ostatnich dwóch miesięcy. W związku z tym w odniesieniu do swoich dwóch rachunków bankowych prowadzonych przez dwóch różnych dostawców usług płatniczych prowadzących rachunek prosi o podanie informacji o wszystkich transakcjach z ostatnich dwóch miesięcy, ze wskazaniem kwoty transakcji, daty wykonania i nazwy odbiorcy, a następnie zaznacza odpowiednie pola w interfejsie użytkownika HappyPayments.

Następnie HappyPayments rozpoczyna procedurę żądania od odpowiednich dostawców usług płatniczych prowadzących rachunek wyłącznie tych informacji, które odpowiadają polom zaznaczonym przez użytkownika A i dotyczą wyłącznie okresu ostatnich dwóch miesięcy. Informacje, takie jak „tytuł” przelewu lub nawet IBAN, nie są wymagane, ponieważ użytkownik A nie prosił o nie.

Aby umożliwić HappyPayments wywiązanie się z obowiązków w zakresie minimalizacji danych, dostawcy usług płatniczych prowadzący rachunek pozwalają HappyPayments na żądanie określonych pól w danym przedziale czasowym.

65. W tym względzie należy również zauważyć, że zgodnie z PSD2 dostawcy usług płatniczych prowadzący rachunek mogą zapewniać dostęp wyłącznie do informacji o rachunku płatniczym. Na

mocy tej dyrektywy nie ma podstawy prawnej do zapewnienia dostępu do danych osobowych zawartych na innych rachunkach, takich jak rachunki oszczędnościowe, hipoteczne lub inwestycyjne. W związku z tym zgodnie z PSD2 należy wdrożyć środki techniczne w celu zapewnienia, aby dostęp był ograniczony do niezbędnych informacji o rachunku płatniczym.

66. Oprócz gromadzenia jak najmniejszej ilości danych dostawca usług musi również wprowadzić ograniczone okresy przechowywania danych. Dane osobowe nie powinny być przechowywane przez dostawcę usług przez okres dłuższy niż jest to niezbędne w związku z celami wskazanymi przez użytkownika usług płatniczych.

67. Jeżeli umowa pomiędzy osobą, której dane dotyczą, a dostawcą świadczącym usługę dostępu do informacji o rachunku wymaga przekazania danych osobowych stronom trzecim, wówczas można przekazać tylko te dane osobowe, które są niezbędne do wykonania umowy. Należy również wyraźnie poinformować osoby, których dane dotyczą, o przekazaniu danych i o tym, jakie dane osobowe mają być przekazane tej stronie trzeciej.

6.3 Bezpieczeństwo

68. EROD podkreśliła już, że naruszenie finansowych danych osobowych „ma wyraźny wpływ na codzienne życie osób, których dane dotyczą", a jako przykład podała ryzyko oszustw płatniczych[36].

69. W przypadku naruszenia danych finansowych osoba, której dane dotyczą, może być narażona na znaczne ryzyko. W zależności od informacji, które wyciekły, osoby, których dane dotyczą, mogą być narażone na ryzyko kradzieży tożsamości, kradzieży środków znajdujących się na ich rachunkach i innych aktywów. Ponadto istnieje możliwość, że ujawnienie danych o transakcjach będzie wiązało się ze znacznym zagrożeniem dla prywatności, ponieważ dane o transakcjach mogą zawierać odniesienia do wszystkich aspektów życia prywatnego osoby, której dane dotyczą. Jednocześnie dane finansowe są oczywiście cenne dla przestępców, a zatem stanowią atrakcyjny cel.

70. Jako administratorzy dostawcy usług płatniczych są zobowiązani do podjęcia odpowiednich środków w celu ochrony danych osobowych osób, których dane dotyczą (art. 24 ust. 1 RODO). Im wyższe ryzyko związane z czynnością przetwarzania realizowaną przez administratora, tym wyższe standardy bezpieczeństwa należy stosować. W związku z tym, że przetwarzanie danych finansowych wiąże się z wieloma poważnymi zagrożeniami, środki bezpieczeństwa powinny być odpowiednio wysokie.

71. Dostawców usług należy objąć wysokimi standardami, w tym mechanizmami silnego uwierzytelniania klienta oraz wysokimi standardami bezpieczeństwa sprzętu technicznego[37]. Ważne są również inne procedury, takie jak weryfikacja podmiotów przetwarzających pod kątem standardów bezpieczeństwa oraz wdrożenie procedur zapobiegających nieuprawnionemu dostępowi.

6.4 Przejrzystość i rozliczalność

72. Przejrzystość i rozliczalność to dwie podstawowe zasady RODO.

73. W odniesieniu do przejrzystości (art. 5 ust. 1 lit. a) RODO) w art. 12 RODO określono, że administratorzy podejmują odpowiednie środki, aby udzielić wszelkich informacji, o których mowa w art. 13 i 14 RODO. Ponadto w artykule tym wymaga się, aby w zwięzłej, przejrzystej, zrozumiałej

[36] Grupa Robocza Art. 29, Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, WP248 rev.01 - zatwierdzone przez EROD.
[37] Zob. regulacyjny standard techniczny.

i łatwo dostępnej formie udzielić wszelkich informacji lub prowadzić komunikację w sprawie przetwarzania danych osobowych. Informacji udziela się jasnym i prostym językiem, na piśmie lub „w inny sposób, w tym w stosownych przypadkach – elektronicznie". W Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679 opracowanych przez Grupę Roboczą Art. 29 i zatwierdzonych przez EROD, przedstawiono konkretne wytyczne dotyczące zgodności z zasadą przejrzystości w środowiskach cyfrowych.

74. Zgodnie z wyżej wspomnianymi wytycznymi w sprawie przejrzystości na podstawie rozporządzenia 2016/679 art. 11 RODO należy interpretować jako sposób egzekwowania rzeczywistej minimalizacji danych pozostający bez uszczerbku dla wykonywania przez osoby, których dane dotyczą, przysługujących im praw, oraz że należy umożliwić wykonywanie praw osoby, której dane dotyczą, przy pomocy dodatkowych informacji dostarczonych przez tę osobę. Mogą zaistnieć sytuacje, w których administrator przetwarza dane osobowe, co nie wymaga identyfikacji osoby, której dane dotyczą (na przykład w przypadku danych spseudonimizowanych). W takich przypadkach istotny może być również art. 11 ust. 1, ponieważ stanowi on, że administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do RODO.

75. W przypadku usług świadczonych na mocy PSD2 art. 13 RODO ma zastosowanie do danych osobowych zebranych od osoby, której dane dotyczą, a art. 14 ma zastosowanie w przypadku, gdy danych osobowych nie pozyskano od osoby, której dane dotyczą.

76. W szczególności należy poinformować osobę, której dane dotyczą, o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu, a także, w stosownych przypadkach, o uzasadnionych interesach realizowanych przez administratora lub ewentualną stronę trzecią. Jeżeli przetwarzanie danych odbywa się na podstawie zgody, o której mowa w art. 6 ust. 1 lit. a) RODO, lub wyraźnej zgody, o której mowa w art. 9 ust. 2 lit. a) RODO, należy poinformować osobę, której dane dotyczą, o istnieniu prawa do cofnięcia zgody w dowolnym momencie.

77. Administrator udziela informacji osobie, której dane dotyczą, mając na uwadze konkretne okoliczności przetwarzania danych osobowych. Jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą[38] – co prawdopodobnie będzie miało miejsce w przypadku dostawców świadczących usługę dostępu do informacji o rachunku – informacje muszą zostać udzielone najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą. Jeżeli planuje się ujawnić dane osobowe innemu odbiorcy, informacje muszą zostać udzielone najpóźniej przy ich pierwszym ujawnieniu.

78. W odniesieniu do usług płatniczych online we wspomnianych wytycznych wyjaśniono, że administratorzy mogą przyjąć warstwowe podejście, jeżeli chcą połączyć różne metody w celu zapewnienia przejrzystości. Zaleca się w szczególności, aby korzystano z warstwowych oświadczeń o ochronie prywatności/warstwowych informacji o polityce prywatności w celu odsyłania do różnych kategorii informacji, które należy podać osobie, której dane dotyczą, zamiast wyświetlać na ekranie wszystkie te informacje w formie ciągłego tekstu, aby nie przytłoczyć użytkownika informacjami, a jednocześnie zapewnić skuteczność informacji.

79. We wspomnianych wytycznych wyjaśniono również, że administratorzy mogą postanowić, że zastosują dodatkowe narzędzia w celu przekazania informacji poszczególnym osobom, których dane dotyczą, takie jak pulpity nawigacyjne prywatności. Pulpit nawigacyjny prywatności jest

[38] Art. 14 ust. 3 lit. b) RODO.

jednym punktem, z którego osoby, których dane dotyczą, mogą przeglądać informacje na temat ochrony prywatności i zarządzać swoimi preferencjami w zakresie prywatności, zezwalając na określone sposoby wykorzystania danych, które ich dotyczą, przez przedmiotowego administratora albo uniemożliwiając takie wykorzystanie[39]. Pulpit nawigacyjny prywatności mógłby zapewnić przegląd dostawców usług będących osobami trzecimi, którzy uzyskali wyraźną zgodę osób, których dane dotyczą, oraz mógłby również oferować odpowiednie informacje na temat charakteru i ilości danych osobowych, do których dostęp uzyskali dostawcy usług będący osobami trzecimi. Dostawca usług płatniczych prowadzący rachunek może co do zasady oferować użytkownikowi możliwość wycofania określonej wyraźnej zgody, o której mowa w PSD2[40], za pośrednictwem przeglądu, co skutkowałoby odmową dostępu do jego rachunków płatniczych jednemu dostawcy usług będącemu osobą trzecią lub większej ich liczbie. Użytkownik może również zwrócić się do dostawcy usług płatniczych prowadzącego rachunek o odmówienie dostępu do jego rachunku płatniczego (rachunków płatniczych) jednemu konkretnemu dostawcy usług będącemu osobą trzecią lub większej ich liczbie[41], ponieważ użytkownik ma prawo do (nie)korzystania z usługi dostępu do informacji o rachunku. Jeżeli w celu udzielenia lub wycofania wyraźnej zgody stosuje się pulpity nawigacyjne prywatności, powinny one być zaprojektowane i stosowane zgodnie z prawem, a w szczególności powinny one zapobiegać tworzeniu przeszkód dla prawa dostawców usług będących osobami trzecimi do świadczenia usług zgodnie z PSD2. W tym względzie i zgodnie z obowiązującymi przepisami PSD2 dostawca usług będący osobą trzecią ma możliwość ponownego uzyskania wyraźnej zgody od użytkownika po jej wycofaniu.

80. Zasady rozliczalności wymagają od administratora ustanowienia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia, aby przetwarzanie odbywało się zgodnie z RODO, w szczególności z głównymi zasadami ochrony danych przewidzianymi w art. 5 ust. 1, a także w celu umożliwienia wykazania, że przetwarzanie jest zgodne z RODO. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, a w razie potrzeby muszą być poddawane przeglądowi i aktualizowane[42].

6.5 Profilowanie

81. Przetwarzanie danych osobowych przez dostawców usług płatniczych może wiązać się z „profilowaniem", o którym mowa w art. 4 pkt 4 RODO. Na przykład dostawcy świadczący usługę dostępu do informacji o rachunku mogą polegać na zautomatyzowanym przetwarzaniu danych osobowych w celu oceny niektórych czynników osobowych osoby fizycznej. W zależności od specyfiki usługi można by ocenić osobistą sytuację finansową osoby, której dane dotyczą. Usługi dostępu do informacji o rachunkach, które mają być świadczone na żądanie użytkowników, mogą obejmować szeroko zakrojoną ocenę danych dotyczących osobistych rachunków płatniczych.

[39] Zgodnie z Wytycznymi Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679 – zatwierdzonymi przez EROD – pulpity nawigacyjne prywatności są szczególnie przydatne w przypadku korzystania przez osoby, których dane dotyczą, z tej samej usługi na różnych urządzeniach, ponieważ zapewniają im dostęp do ich danych osobowych i kontrolę nad tymi danymi bez względu na sposób korzystania z usługi. Umożliwienie osobom, których dane dotyczą, ręcznego dostosowania ustawień prywatności za pośrednictwem pulpitu nawigacyjnego prywatności może również ułatwić spersonalizowanie oświadczenia o ochronie prywatności / informacji o polityce prywatności poprzez uwzględnienie jedynie tych rodzajów przetwarzania, które mają miejsce w przypadku danej osoby.

[40] Zob. np. „wyraźna zgoda", o której mowa w art. 67 ust. 2 lit. a) drugiej dyrektywy w sprawie usług płatniczych.

[41] Zob. także EBA/OP/2020/10, pkt 45.

[42] Art. 5 ust. 2 i art. 24 RODO.

82. Zachowanie administratora wobec osoby, której dane dotyczą, musi być również przejrzyste w kwestii istnienia zautomatyzowanego podejmowania decyzji, w tym profilowania. W tych przypadkach administrator musi przedstawić istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) oraz motyw 60)[43]. Podobnie, zgodnie z art. 15 RODO, osoba, której dane dotyczą, ma prawo zażądać od administratora informacji o istnieniu zautomatyzowanego podejmowania decyzji, w tym o profilowaniu, informacji o zasadach ich podejmowania i konsekwencjach dla osoby, której dane dotyczą, oraz ma prawo uzyskać takie informacje, a także, w pewnych okolicznościach, ma prawo do sprzeciwu wobec profilowania, niezależnie od tego, czy ma miejsce wyłącznie zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach w oparciu o profilowanie[44].

83. Ponadto w tym kontekście istotne jest również prawo osoby, której dane dotyczą, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, zgodnie z art. 22 RODO. Norma ta obejmuje również, w pewnych okolicznościach, konieczność wdrożenia przez administratorów odpowiednich środków ochrony praw osób, których dane dotyczą, takich jak szczegółowe informacje dla osób, których dane dotyczą, prawo do uzyskania interwencji ludzkiej w procesie podejmowania decyzji oraz do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Jak stwierdzono również w motywie 71 RODO, oznacza to m.in., że osoby, których dane dotyczą, mają prawo nie podlegać decyzji, takiej jak automatyczne odrzucenie elektronicznego wniosku kredytowego bez interwencji ludzkiej[45].

84. Zautomatyzowane podejmowanie decyzji, w tym profilowanie, w toku którego dochodzi do przetwarzania szczególnych kategorii danych osobowych, uznaje się za dopuszczalne wyłącznie w przypadku łącznego spełnienia warunków określonych w art. 22 ust. 4 RODO:

- istnieje możliwość zastosowania odstępstwa, o którym mowa w art. 22 ust. 2;
- oraz zastosowanie ma art. 9 ust. 2 lit. a) lub g) RODO. W obydwu przypadkach administrator ustanawia odpowiednie środki zapewniające osobie, której dane dotyczą, poszanowanie jej praw i wolności oraz prawnie uzasadnionych interesów[46].

85. Należy również przestrzegać wymogów dotyczących dalszego przetwarzania, jak określono w niniejszych wytycznych. Wyjaśnienia i instrukcje dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania podane przez Grupę Roboczą Art. 29 w zatwierdzonych przez EROD Wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679, są w pełni istotne w kontekście usług płatniczych i dlatego należy je należycie rozważyć.

W imieniu Europejskiej Rady Ochrony Danych

[43] Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, GR 260 rev. 01 – zatwierdzone przez EROD.

[44] Wytyczne Grupy Roboczej Art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679, WP251rev.01.

[45] Motyw 71 RODO.

[46] Wytyczne Grupy Roboczej Art. 29, w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679, WP251rev.01, s. 24.

Przewodnicząca

(Andrea Jelinek)