

# Zalecenia



**Zalecenia 02/2021 w sprawie podstawy prawnej  
przechowywania danych kart kredytowych wyłącznie w celu  
ułatwienia dokonywania dalszych transakcji online**

**Przyjęte 19 maja 2021 r.**

## Europejska Rada Ochrony Danych

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 jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

### PRZYJĘŁA NASTĘPUJĄCE ZALECENIA:

1. W czasie pandemii COVID-19 gospodarka cyfrowa i handel elektroniczny stale się rozwijały. Analogicznie wzrosło ryzyko korzystania z danych kart kredytowych w Internecie. Jak stwierdziła Grupa Robocza Art. 29 w wytycznych dotyczących oceny skutków dla ochrony danych, naruszenie danych kart kredytowych „*ma wyraźny wpływ na codzienne życie osób, których dane dotyczą*”, ponieważ dane finansowe mogą zostać wykorzystane do „*oszustw płatniczych*”<sup>1</sup>.
2. W tym celu bardzo ważne jest, aby administratorzy wprowadzili odpowiednie zabezpieczenia dla osób, których dane dotyczą, oraz aby zapewnić im kontrolę nad swoimi danymi osobowymi, aby zmniejszyć ryzyko niezgodnego z prawem przetwarzania i zwiększyć zaufanie do środowiska cyfrowego. EROD uważa, że zaufanie to ma zasadnicze znaczenie dla zrównoważonego wzrostu gospodarki cyfrowej.
3. W związku z tym niniejsze zalecenia mają na celu zachęcenie do zharmonizowanego stosowania przepisów o ochronie danych w odniesieniu do przetwarzania danych kart kredytowych w Europejskim Obszarze Gospodarczym (EOG) oraz zagwarantowanie jednolitej ochrony praw osób, których dane dotyczą, przy pełnym poszanowaniu podstawowych zasad ochrony danych, zgodnie z wymogami RODO.
4. W szczególności zalecenia te dotyczą przechowywania danych kart kredytowych przez internetowych dostawców towarów i usług wyłącznie w konkretnym celu, jakim jest ułatwienie dokonywania dalszych zakupów przez osoby, których dane dotyczą<sup>2</sup>. Dotyczą one sytuacji, w której osoba, której dane dotyczą, kupuje produkt lub płaci za usługę za pośrednictwem strony internetowej lub aplikacji oraz przekazuje dane swojej karty kredytowej, zazwyczaj na specjalnym formularzu, w celu zawarcia tej konkretnej transakcji.

---

<sup>1</sup> 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.

<sup>2</sup> Należy pamiętać, że nie obejmują one instytucji płatniczych prowadzących działalność w ramach sklepów internetowych ani organów publicznych. Nie dotyczą również przechowywania danych kart kredytowych w jakimkolwiek innym celu, na przykład wykonania zobowiązania prawnego lub zlecenia powtarzających się płatności w przypadku umów tworzących ciągły stosunek zobowiązaniowy lub abonamentu za usługi długoterminowe (np. umowa na dostawę określonego towaru w każdym miesiącu lub abonament za korzystanie z kanału muzycznego lub serwisu streamingowego do oglądania filmów).

5. Podobnie jak w przypadku każdego przetwarzania, administrator musi mieć ważną podstawę prawną przewidzianą w art. 6 RODO, aby móc przechowywać te dane. W tym względzie należy zauważyć, że niektóre podstawy prawne wymienione w art. 6 RODO nie miałyby zastosowania do tej sytuacji i należy je wykluczyć. Przechowywanie danych kart kredytowych po dokonaniu transakcji, mającego na celu ułatwienie dokonywania dalszych zakupów, nie można uznać za niezbędne do wypełnienia obowiązku prawnego (art. 6 ust. 1 lit. c) RODO) ani do ochrony żywotnych interesów osoby fizycznej (art. 6 ust. 1 lit. d) RODO). Nie można również uznać za odpowiednią podstawę prawną wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e) RODO).
6. Ponadto przechowywanie danych kart kredytowych po dokonaniu płatności za towary lub usługi nie jest samo w sobie niezbędne do wykonania umowy (art. 6 ust. 1 lit. b) RODO). Chociaż przetwarzanie danych związanych z kartą kredytową wykorzystywanych przez klienta do dokonania płatności jest niezbędne przede wszystkim do wykonania umowy, uruchamiając tym samym procedurę przewidzianą w art. 6 ust. 1 lit. b) RODO, przechowywanie tych danych jest przydatne jedynie w celu ułatwienia dokonania potencjalnej kolejnej transakcji i ułatwienia sprzedaży. Takiego celu nie można uznać za absolutnie niezbędny do wykonania umowy na dostawę towarów lub usług, za które osoba, której dane dotyczą, już zapłaciła<sup>3</sup>.
7. Jeżeli chodzi o przetwarzanie niezbędne do celów prawnie uzasadnionego interesu administratora lub osoby trzeciej<sup>4</sup>, EROD zauważa, że aby administrator mógł powołać się na art. 6 ust. 1 lit. f) RODO, muszą zostać spełnione trzy warunki określone w tym artykule<sup>5</sup>. Ta podstawa prawna, po pierwsze, przewiduje konieczność określenia i kwalifikacji uzasadnionego interesu administratora lub osoby trzeciej. Interes administratora lub osoby trzeciej może mieć większy zakres niż cel przetwarzania i musi być obecny i skuteczny w dniu przetwarzania danych<sup>6</sup>.
8. Po drugie, podstawa prawna prawnie uzasadnionego interesu przewiduje konieczność przetwarzania danych osobowych do celów prawnie uzasadnionego interesu. Jeżeli chodzi o ten ostatni warunek, o ile administrator ma uzasadniony interes, o którym mowa powyżej, nie można zdecydowanie stwierdzić, że przechowywanie danych kart kredytowych w celu ułatwienia dokonywania przyszłych zakupów jest niezbędne do celów tego uzasadnionego interesu. Faktyczne dokonanie innego zakupu zależy bowiem od wyboru konsumenta, a nie od możliwości dokonania go „za pomocą jednego kliknięcia”.
9. Ponadto trzeci warunek przewiduje konieczność przeprowadzenia testu równowagi: prawnie uzasadniony interes administratora lub osoby trzeciej musi być wyważony z interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą, w tym z prawem osoby, której

---

<sup>3</sup> Zob. także Wytyczne 2/2019 EROD w sprawie przetwarzania danych osobowych zgodnie z art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online osobom, których dane dotyczą, w szczególności s. 10.

<sup>4</sup> Zob. Opinię Grupy Roboczej Art. 29 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, aktualnie nowelizowaną przez EROD (zob. Program prac EROD na 2021/2022 przyjęty w dniu 16 marca 2021 r.).

<sup>5</sup> Zob. wyrok TSUE z dnia 4 maja 2017 r., Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde przeciwko Rīgas pašvaldības SIA „Rīgas satiksme”, sprawa C-13/16, ECLI:EU:C:2017:336, pkt 28.

<sup>6</sup> Zob. wyrok TSUE z dnia 11 grudnia 2019 r., TK przeciwko Asociația de Proprietari bloc M5A-ScaraA, sprawa C-708/18, ECLI:EU:C:2019:1064, pkt 44.

dane dotyczą, do ochrony danych osobowych i prywatności. W teście równowagi należy uwzględnić szczególne okoliczności przetwarzania<sup>7</sup>. Zasadniczym elementem testu równowagi jest potencjalny wpływ przetwarzania na prawa i wolności osoby, której dane dotyczą<sup>8</sup>. Wpływ ten może zależeć od charakteru danych, konkretnych metod przetwarzania i dostępu stron trzecich do takich danych. Jeśli chodzi o charakter kryterium danych, należy zauważyć, że dane finansowe zostały zakwalifikowane przez Grupę Roboczą Art. 29 jako dane o charakterze wysoce osobistym, ponieważ ich naruszenie ma wyraźny wpływ na codzienne życie osób, których dane dotyczą<sup>9</sup>. W związku z tym, niezależnie od spoczywającego na administratorze obowiązku wdrożenia środków technicznych i organizacyjnych w celu zapewnienia odpowiedniego bezpieczeństwa danych kart kredytowych zgodnie z art. 5 ust. 1 lit. f) RODO oraz faktu, że dane te mogą być przechowywane do innych celów, ich przetwarzanie w celu ułatwienia dokonywania dalszych zakupów może wiązać się z rosnącym ryzykiem naruszenia bezpieczeństwa danych kart kredytowych, ponieważ wiąże się ono z przetwarzaniem danych w innych systemach. Kolejnym istotnym elementem testu równowagi, który można wziąć pod uwagę przy ocenie wpływu przetwarzania na osoby, których dane dotyczą, są uzasadnione oczekiwania osób, których dane dotyczą, wynikające z ich relacji z administratorem, kontekstu i celu gromadzenia danych osobowych<sup>10</sup>. Wydaje się jednak, że w momencie dokonania zakupu, przekazując dane karty kredytowej w celu dokonania płatności, osoba, której dane dotyczą, nie oczekuje, aby dane jej karty kredytowej były przechowywane przez okres dłuższy niż ten, który jest niezbędny do zapłaty za zakupione towary lub usługi. W związku z tym, w tym konkretnym kontekście, podstawowe prawa i wolności osoby, której dotyczy ochrona danych, miałyby prawdopodobnie pierwszeństwo przed interesem administratora.

10. Aspekty te prowadzą do wniosku, że zgoda (art. 6 ust. 1 lit. a) RODO) wydaje się jedyną właściwą podstawą prawną zapewniającą zgodność z prawem wyżej opisanego przetwarzania. W celu wyeliminowania ryzyka związanego z bezpieczeństwem informacji, umożliwienia osobie, której dane dotyczą, sprawowania kontroli nad jej danymi oraz aktywnego decydowania o wykorzystaniu danych jej karty kredytowej, należy uzyskać od osoby, której dane dotyczą, konkretną zgodę przed rozpoczęciem przechowywania jej danych karty kredytowej po dokonaniu zakupu. Zgoda ta umożliwi administratorowi wykazanie chęci osoby fizycznej do ułatwienia dokonywania dalszych zakupów za pośrednictwem konkretnej strony internetowej lub aplikacji, czego nie można domniemywać na podstawie samego faktu dokonania przez tę osobę jednej lub kilku pojedynczych transakcji.
11. Zgoda ta nie może być domniemana, musi być dobrowolna, konkretna, świadoma i jednoznaczna<sup>11</sup>. Musi zostać udzielona w drodze wyraźnego działania potwierdzającego i powinna być wymagana w sposób przyjazny dla użytkownika, np. za pomocą pola, które nie powinno być wcześniej

---

<sup>7</sup> Zob. wyrok TSUE z dnia 24 listopada 2011 r., Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado, sprawy C-468/10 i C-469/10, ECLI:EU:C:2011:777, pkt 47 i 48; wyrok TSUE z dnia 19 października 2016 r., Patrick Breyer przeciwko Bundesrepublik Deutschland, sprawa C-582/14, ECLI:EU:C:2016:779, pkt 62.

<sup>8</sup> Zob. wyżej wspomniany wyrok TSUE z dnia 24 listopada 2011 r., pkt 44; wyżej wspomniany wyrok TSUE z dnia 11 grudnia 2019 r., pkt 56.

<sup>9</sup> 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.

<sup>10</sup> Zob. motyw 47 RODO.

<sup>11</sup> Zob. wytyczne 05/2020 EROD w sprawie zgody na mocy rozporządzenia 2016/679.

zaznaczone<sup>12</sup>, bezpośrednio na formularzu wykorzystywanym na potrzeby gromadzenia danych. Tej konkretnej zgody nie należy mylić ze zgodą udzieloną w odniesieniu do warunków świadczenia usług lub sprzedaży i nie może ona być warunkiem dokonania transakcji.

12. Zgodnie z art. 7 ust. 3 RODO osoba, której dane dotyczą, ma prawo wycofać swoją zgodę na przechowywanie danych karty kredytowej w celu ułatwienia dokonywania dalszych zakupów w dowolnym momencie. Wycofanie zgody musi być równie dobrowolne, proste i łatwe dla osoby, której dane dotyczą jak jej wyrażenie. Musi to prowadzić do skutecznego usunięcia przez administratora danych kart kredytowych przechowywanych wyłącznie w celu ułatwienia dokonywania dalszych transakcji.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

---

<sup>12</sup> Tamże.