

Newsletter

RODO

MAJ 2022 / N° 8

W NUMERZE:

- str.2** Wspólna opinia EIOD oraz EROD w sprawie Data Act
- 4** Wytyczne w sprawie *dark patterns*
- 6** Wyrok WSA: „Administrator nie może być wyręczany w realizacji swoich obowiązków”
- 8** Data Governance Act
- 11** Oświadczenie EROD dotyczące porozumienia ws. nowych Transatlantyckich Ram Ochrony Prywatności Danych

Wspólna opinia EIOD oraz EROD w sprawie Data Act

5 maja Europejska Rada Ochrony Danych („EROD”) oraz Europejski Inspektor Ochrony Danych („EIOD”) opublikowali wspólną opinię w sprawie Data Act.



Data Act to projekt unijnego rozporządzenia, które ma na celu ustanowienie zharmonizowanych przepisów dotyczących dostępu do danych generowanych przez szeroki zakres produktów i usług (w tym produktów i usług należących do Internetu Rzeczy), a także ich wykorzystywania. Co istotne, Data Act ma również na celu wzmocnienie prawa podmiotów danych opisanego w art. 20 RODO, tj. prawa do przenoszenia danych.

Opinia EROD i EIOD

EIOD i EROD zalecają ustawodawcom wprowadzenie ograniczeń lub restrykcji dotyczących wykorzystywania danych wygenerowanych w wyniku korzystania z produktu lub usługi przez jakikolwiek podmiot inny niż osoby, których dane dotyczą, w szczególności w przypadku, gdy przedmiotowe dane mogą pozwolić na wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego osób, których dane dotyczą, lub w inny sposób wiązałyby się z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą. EIOD i EROD wskazują również na potrzebę wprowadzenia wyraźnych ograniczeń dotyczących wykorzystywania odpowiednich danych do

celów marketingu bezpośredniego lub reklamy, monitorowania pracowników, obliczania i modyfikowania składek ubezpieczeniowych oraz oceny zdolności kredytowej. Ograniczenia w wykorzystywaniu danych powinny być również przewidziane w celu ochrony osób, których dane dotyczą, szczególnie osób nieletnich.

EIOD i EROD wyrażają też głębokie obawy co do zgodności z prawem, konieczności i proporcjonalności obowiązku udostępniania danych organom sektora publicznego państw członkowskich UE oraz instytucjom, organom, urzędom i agencjom UE (EUI) w przypadku „wyjątkowej potrzeby”. We wspólnej opinii EIOD i EROD podkreślają, że wszelkie ograniczenia prawa do ochrony danych osobowych wymagają podstawy prawnej, która jest odpowiednio dostępna i przewidywalna. Podstawa prawna musi również określać zakres i sposób wykonywania uprawnień przez właściwe organy oraz muszą jej towarzyszyć zabezpieczenia chroniące osoby, których dane dotyczą, przed arbitralną ingerencją. EIOD i EROD wzywają ustawodawców do znacznie bardziej rygorystycznego zdefiniowania „nagłej sytuacji” lub „wyjątkowej potrzeby” oraz tego, które organy sektora publicznego i instytucje UE powinny mieć możliwość zwracania się o dane.

Z opinią mogą się Państwo zapoznać [TUTAJ](#).

Będziemy informować Państwa na bieżąco o dalszych pracach nad Data Act i działaniach jakie warto podjąć w celu osiągnięcia zgodności z tym unijnym rozporządzeniem.



Wytyczne w sprawie *dark patterns*

2 maja 2022 r. EROD zakończyła przyjmowanie uwag do Wytycznych 03/2022 w sprawie tzw. *dark patterns* w interfejsach platform społecznościowych: Jak je rozpoznawać i jak ich unikać.

Dark patterns są to wszelkiego rodzaju utrudnienia dla użytkownika, w postaci celowo zaprojektowanego interfejsu, które utrudniają podejmowanie klarownych decyzji w trakcie korzystania ze stron internetowych lub ułatwiają wykonanie akcji niekorzystnych.

Mogą to być między innymi domyślnie zaznaczone zgody na dodatkowe usługi marketingowe, eksponowanie przycisku „akceptuj”, przy jednoczesnym zmniejszeniu i ukryciu opcji przeciwnej czy dobranie palety kolorów sugerującej, że brak zgody będzie wiązał się z brakiem możliwości korzystania ze strony.

Wartym odnotowania jest to, że *dark patterns* to zabiegi celowe, czyli niewynikające z braku umiejętności, ale nastawione na uzyskiwanie konkretnych zysków przez autorów.

Kategorie *dark patterns*

Wytyczne EROD wprowadzają 6 kategorii, które pomogą w usystematyzowaniu różnych kategorii wzorów interfejsu, stosowanych najczęściej w mediach społecznościowych, wśród których znajdują się:

1. **Przeciążenie** – konfrontowanie użytkowników ze zbyt dużą ilością żądań informacji lub dawanie zbyt dużej ilości opcji w celu skłonienia ich do udostępnienia większej ilości danych niż jest to wymagane lub niezamierzonego wyrażenia zgody na przetwarzanie.
2. **Pomijanie** – zakłada projektowanie interfejsu w taki sposób, żeby użytkownicy nie zwrócili uwagi na niektóre lub wszystkie aspekty ochrony

- swoich danych.
3. **Podburzanie** – wykorzystuje reakcje emocjonalne użytkownika w celu skłonienia go do udostępnienia swoich danych.
 4. **Utrudnianie** – interfejs projektowany jest w sposób, który utrudnia lub uniemożliwia zarządzanie swoimi danymi w poprawny i przejrzysty sposób.
 5. **Zmienność** – interfejs jest niespójny i nieprzejrzysty, który nie daje użytkownikom klarownych opcji do zarządzania swoimi danymi.
 6. **Pozostawienie w niewiedzy** – interfejs celowo ukrywa narzędzia do zarządzania danymi lub pozostawia użytkowników w niepewności co do przetwarzania danych i możliwości, które mają w związku z wpływaniem na ich przetwarzanie.

Wytyczne EROD

Wytyczne zawierają przykłady z każdej kategorii, które obrazują przypadki niepoprawnego projektowania interfejsu, ale także przedstawiają dobre praktyki, które można wykorzystać chcąc dostosować stronę do standardów wyznaczonych przez RODO.

Warto zaznaczyć, że wytyczne same w sobie nie przewidują konkretnych sankcji za dane przewinienia – jest to już regulowane przez przepisy RODO. Celem dokumentu jest natomiast zaznajomienie osób odpowiedzialnych za interfejs strony internetowej z tym jakie praktyki mogą zostać uznane za naruszenie przepisów dotyczących ochrony danych i prowadzić do sankcji ze strony odpowiedniego organu – w Polsce jest nim Urząd Ochrony Danych Osobowych.

Podstawą prawną do ukarania podmiotów korzystających z *dark patterns* jest Artykuł 5 RODO, a dokładnie wymieniona w nim zasada przejrzystości. Zgodnie z nią, dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

Z treścią wytycznych mogą Państwo zapoznać się **TUTAJ**.



Wyrok WSA: „Administrator nie może być wyręczany w realizacji swoich obowiązków”

Wojewódzki Sąd Administracyjny w Warszawie („WSA”) oddalił skargę Prezesa Sądu Rejonowego w Zgierzu („Prezes Sądu”) na decyzję Prezesa Urzędu Ochrony Danych Osobowych („PUODO”) o nałożeniu kary pieniężnej w wysokości 10 tys. zł za naruszenie RODO.

W przedmiotowej sprawie, kurator sądowy zgubił niezaszyfrowany nośnik pamięci, na którym przechowywane były dane 400 osób objętych nadzorem kuratorskim i wywiadem środowiskowym. PUODO wymierzył karę Prezesowi Sądu, który nie wywiązał się z obowiązków administratora danych. Decyzja ta została zaskarżona.

WSA w uzasadnieniu wyroku z dnia 15 lutego 2022 r. w sprawie o sygn. II SA/Wa 3309/21, uznał że stan faktyczny ustalony przez PUODO był prawidłowy, a materiał dowodowy został odpowiednio oceniony. WSA stwierdził, że w przedstawionej sytuacji naruszenie ochrony danych osobowych było bezsporne – administrator (czyli Prezes Sądu) wydał niezabezpieczone

urządzenie i zobowiązał kuratorów do zabezpieczenia nośnika we własnym zakresie – co stanowiło naruszenie art. 24 RODO, gdyż jest to obowiązek administratora.

PUODO wskazał, że pracownik może nie być odpowiednio wykwalifikowany w zakresie stosowania odpowiednich środków organizacyjnych czy technicznych albo może wdrożyć nieodpowiednie i nieadekwatne zabezpieczenia do zakresu przetwarzanych danych.

Według PUODO naruszone zostały zasady poufności i integralności danych osobowych, co umożliwiło osobom nieuprawnionym dostęp do danych osobowych. WSA zwrócił uwagę, że proces wdrażania zabezpieczeń przyjęty przez Prezesa Sądu pozbawia administratora dostępu do podstawowych informacji, co skutkuje brakiem wiedzy, jakie zabezpieczenia funkcjonują w organizacji i czy zapewniają one odpowiednią skuteczność względem potencjalnych zagrożeń.

WSA oddalił skargę Prezesa Sądu, przyznając, że nałożona administracyjna kara pieniężna spełni funkcję represyjną i prewencyjną.



Data Governance Act

6 kwietnia Parlament Europejski przyjął projekt rozporządzenia w sprawie zarządzania danymi – Data Governance Act („DGA”).



To przełomowy moment dla rozwoju sztucznej inteligencji w obszarze Unii Europejskiej – DGA jest jednym z kluczowych filarów europejskiej strategii w zakresie danych, mającym zwiększyć możliwość łatwiejszej wymiany danych i przyczynić się do stworzenia jednolitego rynku danych.

Cele DGA

DGA ma na celu przede wszystkim:

- Umożliwić obywatelom UE możliwość decydowania co dzieje się z ich danymi;
- Ułatwić udostępnianie danych między przedsiębiorstwami, co przyczyni się do większej innowacyjności w zakresie rozwoju AI;
- Ułatwić proces dobrowolnego udostępniania danych przez przedsiębiorstwa, ale też osoby prywatne na rzecz rozwoju społeczeństwa jako ogółu;
- Udostępnić osobom fizycznym pomoc w wykonywaniu ich praw wynikających z RODO za sprawą „pośrednika w udostępnianiu danych osobowych”.

Zakładane rozwiązania

Rozdział II daje możliwość organom sektora publicznego udostępnianie zebranych danych, które są chronione przepisami prawa, po odpowiednim przetworzeniu takim jak anonimizacja czy usunięcie informacji poufnych. Co ważne zasady dostępu do tego typu danych muszą być ogólnodostępne i niedyskryminujące, przewidziano też zakaz zawierania umów, które miałyby prowadzić do uzyskania wyłączności dostępu do danych przez podmiot zewnętrzny.

Rozdział III definiuje instytucję dostawców usług udostępniania danych, które to usługi mają polegać na pośredniczeniu między posiadaczami danych a potencjalnymi użytkownikami. DGA pozwala na podjęcie szerokiego wachlarza działań, między innymi tworzenie infrastruktury do wymiany lub wspólnego wykorzystywania danych, zarządzanie bazami danych i specjalnymi platformami. Warto zaznaczyć, że dostawcy nie mogą sami wykorzystywać danych, w odniesieniu do których świadczą usługi.

Zawarte w rozdziale IV altruistyczne podejście do danych obejmuje rejestrację podmiotów, które zamierzają działać z zamiarem realizacji celów korzystnych dla ogółu społeczeństwa, bez nastawienia na indywidualny zysk.

Planowane jest utworzenie Europejskiej Rady ds. Innowacji w zakresie Danych.



Kto skorzysta?

Planowane udogodnienia przewidziane w DGA będą najlepiej dostrzegalne w następujących sektorach:

- **Służbie zdrowia** – lepsza jakość opieki zdrowotnej i większa personalizacja według potrzeb pacjenta. Dzięki wymianie danych przyspieszono proces opanowania COVID-19.
- **Środowisku naturalnym** – lepszy przepływ danych umożliwi skuteczniejsze zwalczanie klęsk żywiołowych, a także przyczyni się do redukcji emisji CO2 i spowolni zmiany klimatyczne.
- **Rolnictwie i sektorze żywieniowym** – możliwe będzie stworzenie nowych rozwiązań technologicznych i usprawnienie procesów związanych z technologią żywienia.
- **Administracji publicznej** – lepszy dostęp do danych statystycznych przyczyni się do uzyskania lepszego obrazu społeczeństwa na podstawie, którego będą podejmowane decyzje.

Z treścią projektu rozporządzenia mogą Państwo zapoznać się **TUTAJ**.

Oświadczenie EROD dotyczące porozumienia ws. nowych Transatlantyckich Ram Ochrony Prywatności Danych

6 kwietnia 2022 r., podczas 63 plenarnego posiedzenia, EROD przyjęła oświadczenie w sprawie porozumienia dotyczącego nowych Transatlantyckich Ram Ochrony Prywatności Danych (tzw. Tarcza Prywatności 2.0).

Przypomnijmy, że wskazane porozumienie z USA zostało ogłoszone 25 marca przez Komisję Europejską i dotyczy potencjalnej nowej podstawy transferu danych pomiędzy USA a państwami UE, która to zastąpiłaby tzw. Tarczę Prywatności, unieważnioną na skutek wyroku TSUE w sprawie Schrems II w lipcu 2020 r.

Zgodnie z przepisami RODO, Komisja Europejska powinna zasięgnąć opinii EROD przed przyjęciem ewentualnej nowej decyzji stwierdzającej odpowiedni stopień ochrony danych.

EROD zapowiedziała, że przeanalizuje, jak ww. porozumienie przekłada się na konkretne propozycje prawne, zapewniające pewność prawną osobom fizycznym z EOG i podmiotom przekazującym dane. EROD skupi się zwłaszcza na analizie, czy zbieranie danych osobowych do celów bezpieczeństwa narodowego jest ograniczone do tego, co jest bezwzględnie niezbędne i proporcjonalne.

Z oświadczeniem EROD mogą się Państwo zapoznać [TUTAJ](#).



KONTAKT / AUTORZY



Katarzyna Szczudlik

Partner

katarzyna.szczudlik@ssw.solutions



Aleksandra Czubek

Associate

aleksandra.czubek@ssw.solutions



Karolina Piłkuła

Associate

karolina.pikula@ssw.solutions