SK&S PRIVACY INSIGHT

Kwartalnik o prawie ochrony danych osobowych

SOŁTYSIŃSKI KAWECKI SZLĘZAK

W tym numerze

LUTY 2023 | NUMER 3

Szanowni Państwo,

w załączeniu przekazujemy kolejny numer naszego Kwartalnika o prawie ochrony danych osobowych.

Końcówka 2022 r. w tej dziedzinie była bardzo gorąca, zarówno w obszarze legislacji – weszły w życie Akt o usługach cyfrowych i Akt o rynkach cyfrowych, jak i wydawanych decyzji i orzeczeń. Rok 2023 zapowiada się równie pracowicie – na forum UE trwają m.in. prace nad Aktem w sprawie danych, a w Polsce możemy spodziewać się przyjęcia Prawa Komunikacji Elektronicznej. Krótkie podsumowanie działań legislacyjnych znajdą Państwo poniżej. Przedstawiamy również informacje o ostatnich decyzjach UODO i wyrokach sądowych oraz krótkie artykuły dotyczące zmian w zakresie badania trzeźwości pracowników oraz tzw. dark patterns w aplikacjach i wyszukiwarkach internetowych.

Zapraszamy do lektury i życzymy Szczęśliwego Nowego Roku!

Agata Szeliga
Partner

Zmiany w obszarze ochrony danych osobowych w 2023 r.

Rok 2023 zapowiada się na wyjątkowo pracowity dla prawodawców. Poniżej przedstawiamy podsumowanie głównych aktów prawnych dotyczących danych osobowych i prywatności, które mają wejść w życie lub być przedmiotem prac legislacyjnych.

Regulacje na poziomie UE

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE

Akt o usługach cyfrowych
(Digital Service Act)

Usługi pośrednie (zwykły przekaz (mere conduit), caching, hosting). Przepisy obejmą szerokąkategorię usług pośrednich, od prostych stron internetowych po usługi w zakresie infrastruktury internetowej oraz platformy i wyszukiwarki internetowe.

Etap prac:
Zakończony

- **16 listopada 2022 r.** – wejście w życie
- **17 lutego 2024 r.** – od tego momentu przepisy będą obowiązywać w całości, jednak wybrane regulacje będą stosowane już w 2023 r.

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniający niektóre akty ustawodawcze Unii

Wprowadzenie zasad wykorzystywania oprogramowania opartego na modelach wykorzystujących technologię sztucznej inteligencji. Uzupełnienie przepisów dotyczących zautomatyzowanego przetwarzania danych.

Etap prac:
W toku

Nieznana data wejścia w życie.

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828

Akt o rynkach cyfrowych
(Digital Market Act)

Obowiązki tzw. strażników Dostępu (Gatekeepers) tj. największych platform cyfrowych o kluczowej roli na rynku usług cyfrowych.

Etap prac:
Zakończony

- **1 listopada 2022 r.** – wejście w życie
- **2 maja 2023 r.** – początek obowiązywania

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE

(rozporządzenie w sprawie prywatności i łączności elektronicznej, tzw. E-privacy)

Uzupełnienie przepisów RODO w zakresie prywatności online, w tym wykorzystywanie informacji o urządzaniu końcowym użytkownika (np. korzystanie z plików cookies i przypadki w których konieczne jest zbieranie zgody na śledzenie użytkowników za ich pomocą). E-Privacy dotyczy również wykorzystania danych pochodzących z łączności elektronicznej oraz wysyłania komunikatów marketingu bezpośredniego.

Etap prac:
W toku

Nieznana data wejścia w życie.

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014

Wprowadzenie jednolitych wymogów dotyczących bezpieczeństwa sieci i systemów informatycznych wspierających procesy biznesowe podmiotów finansowych, niezbędne do osiągnięcia wysokiego wspólnego poziomu operacyjnej odporności cyfrowej.

Zakres jego obowiązywania krzyżuje się np.: z zakresem Komunikatu Chmurowego UKNF.

Etap prac:
Zakończony

- Wejście w życie **16 stycznia 2023 r.**
- Rozpoczęcie obowiązywania **17 stycznia 2025 r.**

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiej przestrzeni danych dotyczących zdrowia

(EU Health Data Space)

Stworzenie scentralizowanej bazy danych zdrowotnych i wsparcie wykorzystania danych dotyczących zdrowia w całej UE. Także, wzmocnienie praw osób fizycznych w odniesieniu do ich danych osobowych dotyczących zdrowia. Stworzenie systemu umożliwiającego wtórne wykorzystywania elektronicznych danych dotyczących zdrowia dla wskazanych w regulacji celów.

Etap prac:
W toku

Nieznana data wejścia w życie.

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania

(akt w sprawie danych)

Określenie zasad dostępu do danych i przenoszenia danych między operatorami usług chmurowych. Akt określa klauzule zakazane w umowach dotyczących dostępu do danych i dzielenia się danymi.

Etap prac:
W toku

Nieznana data wejścia w życie.

Polskie przepisy

Ustawa o ochronie osób zgłaszających naruszenia prawa

(projekt z dnia 5 stycznia 2023 r.)

Zapewnienie ochrony osobom zgłaszającym lub ujawniającym publicznie informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą.

Etap prac:
W toku - na etapie projektu w Rządowym Centrum Legislacji

Nieznana data wejścia w życie. (planowany termin przyjęcia projektu przez RM: I kwartał 2023 r.)

Prawo Komunikacji Elektronicznej

(PKE)

Zastąpienie w całości Prawa Telekomunikacyjnego, w tym w zakresie zgód na marketing oraz regulacji dot. cookies.

Etap prac:
Ustawa jest po pierwszym czytaniu w Sejmie

Nieznana data wejścia w życie.

Kontrola trzeźwości pracowników oraz praca zdalna w kontekście RODO – nowelizacja Kodeksu Pracy

Sylwia Macura-Targosz
Starszy Prawnik, radca prawny
sylwia.macura-targosz@skslegal.pl
+48 694 415 447

W dniu 13 stycznia 2023 r. Sejm uchwalił ustawę o zmianie ustawy - Kodeks pracy oraz niektórych innych ustaw („**Ustawa**") odrzucając wszystkie poprawki zaproponowane przez Senat. Ustawa czeka na podpis Prezydenta oraz publikację.

Ustawa przyznaje pracodawcom prawo do prowadzenia prewencyjnej kontroli trzeźwości pod kątem zawartości alkoholu oraz substancji działających podobnie jak alkohol jeżeli jest to niezbędne do zapewnienia ochrony życia i zdrowia pracowników oraz innych osób[1] lub ochrony mienia. Kontrola trzeźwości nie może naruszać godności oraz innych dóbr osobistych pracownika i może być prowadzona tylko przy użyciu metod niewymagających badania laboratoryjnego oraz za pomocą urządzenia posiadającego ważny dokument potwierdzający jego kalibrację lub wzorcowanie. Kontroli trzeźwości mogą podlegać nie tylko pracownicy pracujący stacjonarnie, ale również ci którzy pracują w sposób zdalny. Kontrolą objęci mogą być nie tylko pracownicy w rozumieniu kodeksu pracy, ale również osoby zatrudnione na innej podstawie niż umowa o pracę czy prowadzące działalność gospodarczą. Ustawa reguluje również kwestie dotyczące pracy zdalnej.

Jakie regulacje zawiera Ustawa i na co należy zwrócić uwagę w kontekście ochrony danych osobowych?

Kontrola trzeźwości

- Ustawa daje pracodawcom **podstawę prawną do przetwarzania danych osobowych szczególnej kategorii (informacja o trzeźwości jest informacją o stanie zdrowia)**. RODO dopuszcza przetwarzania danych osobowych szczególnej kategorii w przypadku gdy jest to niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora w dziedzinie prawa pracy, o ile jest to dozwolone prawem państwa członkowskiego przy odpowiednim zabezpieczeniu praw podstawowych oraz interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. b RODO).

- Pracodawca może przetwarzać ograniczony **zakres danych**, tj. **datę i czas sporządzenia badania oraz jego wynik**. Informacje te pracodawca powinien dołączyć do akt osobowych pracownika i **co do zasady są one usuwane najpóźniej po upływie roku od dnia ich zebrania** (dłuższy termin obowiązuje w przypadku nałożenia na pracownika kary lub gdy informacje te stanowią dowód w postępowaniu).

- Pracodawca zobowiązany jest **uregulować zasady kontroli trzeźwości na takich samych zasadach, jak w przypadku monitoringu**, a zatem regulacje dotyczące kontroli trzeźwości powinny znaleźć się w układzie zbiorowym pracy, regulaminie pracy lub obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy oraz powinny wskazywać w szczególności na sposób przeprowadzania kontroli, jej częstotliwość, kategorie pracowników objętych kontrolą itp. Pracownicy powinni zostać poinformowani o możliwości prowadzenia takich kontroli nie później niż na 2 tygodnie przed rozpoczęciem ich stosowania, nowi pracownicy przed dopuszczeniem ich do pracy.

- Wprowadzenie kontroli trzeźwości u pracodawcy **wymaga również zmian/aktualizacji dokumentacji dotyczącej ochrony danych osobowych**, w tym:
  - przygotowania upoważnień dla osób przeprowadzających kontrolę trzeźwości w imieniu pracodawcy do przetwarzania związanych z tym danych osobowych oraz zobowiązań do zachowania ich w tajemnicy przez te osoby;
  - zaktualizowanie klauzuli informacyjnej w zakresie nowego procesu przetwarzania danych osobowych;
  - zaktualizowanie rejestru czynności przetwarzania poprzez dodanie nowego procesu oraz polityki retencji;

- Wprowadzenie przez pracodawcę prewencyjnej kontroli trzeźwości powinno być poprzedzone **przeprowadzeniem analizy ryzyka**, a w przypadku stwierdzenia występowania wysokiego ryzyka naruszenia praw lub wolności – również **przeprowadzeniem oceny skutków dla ochrony danych (DPIA)**.

- Konieczność zawarcia umowy powierzenia przetwarzania danych w przypadku powierzenia przeprowadzenia kontroli trzeźwości pracowników podmiotowi zewnętrznemu, np. zewnętrznej firmie ochroniarskiej.

Praca zdalna

- Pracodawca zobowiązany jest do **określenia procedur ochrony danych osobowych** oraz przeprowadzenia – w miarę potrzeby – szkoleń w tym zakresie. Pracownik zobowiązany będzie do potwierdzenia zapoznania się z tymi procedurami oraz do ich stosowania.

- Procedury powinny regulować, w szczególności zasady korzystania ze sprzętu elektronicznego (prywatnego jak i dostarczonego przez pracodawcę), zasady obiegu dokumentacji w firmie (papierowej jak i elektronicznej). Pracodawca będzie zobowiązany do zapewnienia odpowiednich środków celem zapewnienia bezpieczeństwa oraz poufności danych osobowych przetwarzanych w ramach pracy zdalnej.

- Wprowadzenie przez pracodawcę możliwości pracy zdalnej powinno być poprzedzone przeprowadzeniem **analizy ryzyka**, a w przypadku stwierdzenia występowania wysokiego ryzyka naruszenia praw lub wolności – również przeprowadzeniem **oceny skutków dla ochrony danych (DPIA)**.

Ustawa dostępna jest **tutaj** (wersja uchwalona przez Sejm 1 grudnia 2022 r. po rozpatrzeniu poprawek Senatu).

Dark patterns w świetle nowych regulacji

Maciej Jakubowski
Prawnik, radca prawny
maciej.jakubowski@skslegal.pl
+48 882 630 942

Dark patterns – czym są?

Pod pojęciem dark patterns rozumiemy interfejsy i mechanizmy stosowane na stronach internetowych, które prowadzą użytkowników do podejmowania niezamierzonych, niechcianych i potencjalnie szkodliwych decyzji, w tym decyzji dotyczących przetwarzania ich danych osobowych. Poza przepisami o ochronie danych osobowych, dark patterns mogą również naruszać przepisy o ochronie konsumentów.

Przykładami dark patterns może być:

- różne eksponowanie przycisków wyboru (np. zgoda - na zielono, odmowa – na czerwono),

- wielokrotne żądania od odbiorcy usługi dokonania wyboru, w szczególności przez częstotliwe pokazywanie wyskakujących okienek (pop-up),

- prezentowanie „ściany" informacji, aby skłonić do akceptacji określonych praktyk,

- prezentowanie zbyt wielu opcji, które utrudniają dokonanie wyboru lub sprawiają, że użytkownik pomija niektóre ustawienia, W efekcie użytkownik może zrezygnować lub przeoczyć ustawienia dotyczące ochrony danych,

- utrudnianie procesu rezygnacji z subskrypcji w porównaniu z przebiegiem procedury zapisu.

Dark patterns w świetle RODO

Przepisy RODO nie zawierają bezpośrednich regulacji w zakresie dark patterns. Jednak ze swojej natury dark patterns mogą prowadzić do naruszenia podstawowych zasad dotyczących ochrony danych osobowych, w szczególności zasady legalności, transparentności czy zasady rozliczalności (art. 5 ust 1 lit (a) oraz art. 5 ust 2 RODO). Mechanizmy powodujące, że rezygnacja z subskrypcji jest trudniejsza niż zapisanie powodują, że zgoda taka jest wadliwa w świetle art. 7 ust. 3 RODO. Natomiast prezentowanie „ściany teksu" np. w ramach informacji o przetwarzaniu danych osobowych, będzie naruszało obowiązek informowania podmiotów danych w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem (art. 12 RODO). W kontekście dark patterns warto również wspomnieć o zasadzie ochrony danych w fazie projektowania oraz zasady domyślnej ochrony danych (art. 25 RODO). Temat dark patterns w świetle RODO nie był szeroko podejmowany przez organy nadzorcze w wydawanych decyzjach. Nie oznacza to, że problem był zupełnie pomijany. W 2022 r. Europejska Rada Ochrony Danych wydała Wytyczne 3/2022 w sprawie dark patterns w interfejsach platform społecznościowych, w których opisała podstawowe mechanizmy ich działania oraz rekomendacje. Tym niemniej, zdecydowano się na podjęcie bardziej zdecydowanych kroków przez bezpośredni uregulowanie zagadnień dark patterns w nowych przepisach mających stanowić filary rynku cyfrowego w UE.

Dark Patterns a nowe regulacje

Pierwszą z regulacji, która wprost odnosi się do dark patterns jest Akt o usługach cyfrowych (DSA). Zgodnie z art. 25 DSA dostawcy platform internetowych nie mogą projektować, organizować ani obsługiwać swoich interfejsów internetowych w sposób, który wprowadza w błąd odbiorców usługi lub nimi manipuluje lub w inny istotny sposób zakłóca lub ogranicza zdolność odbiorców ich usługi do podejmowania wolnych i świadomych decyzji. Pierwotnie, regulacja ta miała dotyczyć wszystkich dostawców usług pośrednich (tj. usług przekazu, cachingu, hostingu)*. Jednak na skutek przyjętego kompromisu krąg adresatów ograniczono do dostawców platform internetowych. Motyw 67 DSA zawiera pomocną wykładnię dla zrozumienia dark patterns na interfejsach platform internetowych (zwodnicze interfejsy). Jednocześnie zwraca się uwagę, że legalne praktyki, na przykład reklamowe, które są zgodne z prawem Unii, nie powinny same w sobie być uznawane za zwodnicze interfejsy.

Druga z regulacji poruszająca tematykę dark patterns to Akt o rynkach cyfrowych (DMA). Krąg adresatów nowych obowiązków jest ograniczony do strażników dostępu, tj. największych platform cyfrowych o kluczowej roli na rynku usług cyfrowych. DMA wskazuje, że strażnicy dostępu nie powinni dopuszczać się praktyk, które mogłyby podważyć skuteczność zakazów i obowiązków ustanowionych w tym akcie. Takie zachowanie może stanowić przedstawianie użytkownikom końcowym opcji wyboru w sposób, który nie jest neutralny, lub wykorzystywanie struktury, funkcji lub sposobu obsługi interfejsu użytkownika lub jego części w celu osłabienia lub ograniczenia autonomii użytkownika, jego możliwości podejmowania decyzji lub wyboru. Natomiast w motywie 63 DMA wskazano, że należy zakazać strażnikom dostępu niepotrzebnego utrudniania lub komplikowania użytkownikom biznesowym lub użytkownikom końcowym rezygnacji z subskrypcji podstawowej usługi platformowej.

Podsumowanie

Dark patterns są obecne w przestrzeni cyfrowej od lat. Wraz z nowymi przepisami, które bezpośrednio odnoszą się do tych zagadnień oraz dotychczasowymi wytycznymi należy liczyć się z większą aktywnością organów regulacyjnych i zweryfikować stosowane mechanizmy pod kątem zgodności z tymi regulacjami.

* Przykłady usług pośrednich wskazane w motywie 29 DSA: (i) **usługi „zwykłego przekazu"**: punkty wymiany ruchu internetowego, punkty dostępu bezprzewodowego, wirtualne sieci prywatne; **usługi "cachingu"**: zapewnianie sieci dostarczania treści, odwrotnych serwerów proxy lub serwerów proxy adaptacji treści; **usługi „hostingu"**: przetwarzanie w chmurze, web hosting, odpłatne usługi odsyłania czy usługi umożliwiające wymianę informacji i treści online, w tym przechowywanie i udostępnianie plików.

ORZECZNICTWO & DECYZJE

Katarzyna Wnuk
Prawnik, adwokat
katarzyna.wnuk@skslegal.pl
+48 602 151 178

Tablice rejestracyjne nie są danymi osobowymi – kontynuacja dotychczasowej linii orzeczniczej NSA

Naczelny Sąd Administracyjny w wyroku z dnia 3 listopada 2022 r. (sygn. akt III OSK 1522/21) podtrzymał dotychczasowe stanowisko prezentowane przez Naczelny Sąd Administracyjny, zgodnie z którym tablice rejestracyjne pojazdów nie są danymi osobowymi.

Sprawa dotyczyła wniosku o udostępnienie nagrania z wideorejestratora samochodu policyjnego złożonego w trybie dostępu do informacji publicznej. Policja odmówiła udzielenia dostępu to takiego nagrania wskazując, że przedstawia ono wizerunki innych osób kontrolowanych (poza wizerunkiem wnioskodawcy) jak również marki, modele oraz numery rejestracyjne pojazdów, a tym samym udostępnienie nagrania stanowiłoby naruszenia prawa do prywatności tych osób. Wojewódzki Sąd Administracyjny zgodził się z powyższą argumentacją stwierdzając, że *„dysponując numerem rejestracyjnym, marką i kolorem pojazdu można– nie koniecznie w prosty i łatwy sposób (...) – ustalić dane osobowe właściciela pojazdu (...)”*.

Z powyższą argumentacją nie zgodził się Naczelny Sąd Administracyjny, który podzielił stanowisko wyrażone przez NSA w wyroku z dnia 14 maja 2021 r. (sygn. akt III OSK 1466/21), który uznał, że ***„numer rejestracyjny samochodu nie podlega ochronie wynikającej z prawa do prywatności, gdyż identyfikuje samochód, a nie osobę****, odnoszona winna być do standardowych numerów rejestracyjnych składających się z liter i cyfr, niepozwalających na powiązanie samochodu z właścicielem oraz do przypadków, w których samochód z tablicą rejestracyjną znajduje się lub jest prezentowany bez połączenia z innymi informacjami odnoszącymi się do czasoprzestrzeni lub w powiązaniu z innymi danymi, w tym wizerunku osób nim podróżujących”. (...) Tak więc jeżeli definicja „danych osobowych” odnosi się do osób fizycznych – **dane dotyczące rzeczy (samochód) nie stanowią informacji, o których mowa w art. 4 pkt 1 RODO, jeżeli zidentyfikowanie posiadacza tej rzeczy może by dokonane tylko poprzez dostęp do odpowiednych rejestrów lub katalogów.”***

Stanowisko PUODO

Prezes Urzędu Ochrony Danych Osobowych opiniując w 2020 roku zmiany w Prawie o ruchu drogowym zaprezentował odmienne stanowisko. W ocenie PUODO tablice rejestracyjne stanowią dane osobowe właściciela pojazdu, są to bowiem informacje, za pośrednictwem których możliwe jest zidentyfikowanie – w sposób pośredni – osoby będącej właścicielem pojazdu.

Stanowisko PUODO

Stanowisko europejskich organów nadzoru

Odmienne od NSA stanowisko prezentują również europejskie organy nadzoru, w tym brytyjski organ nadzoru **ICO**, francuski organ nadzoru **CNIL**, czy włoski organ nadzoru **GPDP**, które uznają, że tablice rejestracyjne stanowią dane osobowe.

Wyrok NSA z dnia 3 listopada 2022 r.

Brak konieczności weryfikacji renomowanych podmiotów przetwarzających?

Do tej pory w wielu decyzjach PUODO stwierdzał, że jeżeli administrator danych powierza dane osobowe innemu podmiotowi (tj. umożliwia temu podmiotowi przetwarzanie danych w jego imieniu i na jego rzecz, np. w związku ze świadczeniem usług chmurowych lub marketingowych) to konieczne jest zarówno podpisanie odpowiedniej umowy powierzenia, jak i wykonywanie cyklicznych weryfikacji tego podmiotu pod kątem zapewniania przez niego bezpieczeństwa danych. Stwarzało to wyzwanie dla administratorów danych, zwłaszcza małych i średnich firm korzystających ze standardowych usług.

W niedawnym wyroku (wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 19 kwietnia 2022 r. (sygn. II SA/Wa 2259/21)) WSA stwierdził, że administratorzy powierzający dane renomowanym, profesjonalnym podmiotom, zapewniają tym samym stosowanie środków organizacyjnych i technicznych wymaganych przez RODO (w rozważanym przez WSA przypadku za podmiot taki został uznany Microsoft). Z powyższego wynika, że w przypadku zawierania umowy z renomowanym podmiotem, w ramach analizy spełnienia wymogów dotyczących bezpieczeństwa wynikających z RODO wystarczające jest odnotowanie faktu zawarcia umowy oraz czynności podjętych w momencie uruchomienia usługi, a także powołanie się na renomę podmiotu. Oczywiście renoma ta powinna być jednak weryfikowana (np. poprzez sprawdzanie, czy podmiot przetwarzający nie został ukarany za naruszenie przepisów o ochronie danych osobowych).

Należy mieć także na uwadze, że niektóre z powszechnie znanych podmiotów, mogą nie być uznane za renomowane w kontekście ochrony danych osobowych, np. w przypadku wydania decyzji stwierdzające naruszenie przez nie ochrony danych osobowych. Tym samym, oparcie się na renomie podmiotu przetwarzającego powinno wiązać się z bieżącą i uważną weryfikacją rynku oraz powinno być odpowiednio uzasadnione w dokumentacji wewnętrznej.

Wyrok WSA z dnia 19 kwietnia 2022 r.

Jawny Rejestr Beneficjentów Rzeczywistych narusza prawa podstawowe (w tym prawo do ochrony danych osobowych)

Wyrokiem z dnia 22 listopada 2022 r. w sprawach połączonych C-37/20 i C-601/20 Trybunał Sprawiedliwości Unii Europejskiej („TSUE" lub „Trybunał") orzekł nieważność art. 1 pkt. 15 lit. c dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającego art. 30 ust. 5, 5a i 9 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 w zakresie w którym umożliwia udostępnienie przez państwa członkowskie informacji o beneficjentach rzeczywistych każdej osobie.

Zgodnie z brzmieniem Dyrektywy AML państwa członkowskie mają obowiązek zapewnić dostęp do danych o beneficjentach rzeczywistych we wszystkich przypadkach i każdej osobie. Ostateczny zakres danych, które mają być udostępnione pozostawiony został do decyzji państw członkowskich. Dyrektywa umożliwiała udostępnienie ich każdej osobie, również przez upublicznienie.

Trybunał w orzeczeniu podkreślił, że przekazywanie informacji zawartych w rejestrze nieograniczonemu kręgowi adresatów może kolidować z podstawowymi prawami poszanowania życia prywatnego i rodzinnego osób fizycznych (art. 7 Karty praw podstawowych Unii Europejskiej) oraz naruszać prawo do ochrony ich danych osobowych (art. 8 Karty praw podstawowych Unii Europejskiej).

Podkreślono, że publiczne udostępnianie w rejestrze informacji na temat sytuacji materialnej i finansowej osób fizycznych może prowadzić do niewłaściwego wykorzystania takiej wiedzy i stworzenia istotnego zagrożenia dla praw podstawowych beneficjentów rzeczywistych. W ocenie Trybunału udzielenie publicznego dostępu do danych, w celu ochrony interesu publicznego nie jest proporcjonalne w kontekście wyżej opisanych ryzyk naruszenia praw.

Mimo, że uchylając przepisy Dyrektywy komentowany wyrok nie wywołuje bezpośredniego skutku w prawie krajowym, w przyszłości orzeczenie będzie mieć znaczący wpływ na praktykę działania organów prowadzących rejestry beneficjentów rzeczywistych, w tym polskiego Centralnego Rejestru Beneficjentów Rzeczywistych np.: poprzez kształtowanie interpretacji pojęcia interesu prawnego przez organy administracji przy udzielaniu informacji z rejestru. W jurysdykcjach, które w przeciwieństwie do polskiej zdecydowały się prowadzić rejestry publicznie (np.: Luksemburgu), orzeczenie doprowadziło do zmiany istniejącej praktyki regulatora i usunięcia rejestrów z Internetu. Wielu komentatorów uznaje orzeczenie za kontrowersyjne, jako uderzające w zasadę transparentności działań organów i będące krokiem wstecz w rozwoju regulacji dot. przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. W naszej ocenie należy jednak zgodzić się z poglądem, że publiczne ujawnianie pełnego rejestru może doprowadzić do niepotrzebnego naruszenia praw podstawowych osób tam ujawnionych, a oczekiwany efekt dyrektywy może zostać osiągnięty również w przypadku udostępniania rejestru węższemu kręgowi odbiorców lub ograniczenia zakresu udostępnionych informacji.

Wyrok TSUE z dnia 22 listopada 2022 r.

Jakub Derulski
Prawnik, adwokat
jakub.derulski@skslegal.pl
+48 880 780 275

Operator wyszukiwarki musi usunąć linki do informacji, jeżeli osoba żądająca ich usunięcia udowodni, że takie informacje są w oczywisty sposób nieprawdziwe

Sprawa została wszczęta wskutek skierowanej do Google prośby dwóch managerów grupy spółek inwestycyjnych o usunięcie wskazanych linków oraz zdjęć z listy wyników wyszukiwania pojawiającej się po wpisaniu ich imion i nazwisk. Linki objęte prośbą prowadziły do artykułów krytycznych wobec wdrażanego przez grupę modelu inwestycyjnego, co zostało uznane przez ww. managerów za nieprawdziwe. Prośba ta nie została uwzględniona przez Google, które powołało się na kontekst zawodowy treści i niemożliwość ustalenia czy są one prawdziwe, czy nie.

Sprawa ta finalnie trafiła do TSUE, który rozważył ją analizując wzajemną równowagę pomiędzy prawem do wolności wypowiedzi i informacji a prawem do prywatności.

TSUE uznał, że prawo do wolności wypowiedzi i informacji nie może zostać uznane za nadrzędne wobec prawa do prywatności w przypadku, w którym przynajmniej część informacji zawartych pod linkiem okaże się nieprawdziwa i niemająca nikłego znaczenia dla całokształtu treści.

Oczywiście, jak wskazało TSUE, należy pamiętać, że prawo do ochrony danych nie jest prawem bezwzględnym. Co do zasady, prawo do prywatności należy uznać za nadrzędne wobec prawa internautów do dostępu do informacji, niemniej jednak każdą sytuację należy oceniać odrębnie, w świetle szczególnych okoliczności, charakteru informacji, wpływu informacji na prywatność osoby, roli tej osoby w życiu publicznym oraz interesu publicznego w dysponowaniu informacją. W przypadku w którym informacje są nieprawdziwe, można zastosować wskazane powyżej podejście TSUE.

W jaki sposób określa się „nieprawdziwość" informacji?

To osoba żądająca usunięcia linków musi wykazać oczywistą nieprawdziwość treści, która nie ma nikłego znaczenia. **Osoba ta powinna przedstawić jedynie takie dowody, jakich przeprowadzenia można od niej racjonalnie wymagać** – TSUE dążyło do uniknięcia nałożenia zbyt dużego ciężaru na osobę, której dane dotyczą.

Z drugiej strony, jak wskazuje TSUE, operator wyszukiwarki nie może zostać zobowiązany do odgrywania aktywnej roli w przeprowadzaniu dowodów. Operator musi wziąć pod uwagę wszystkie wchodzące w grę prawa i interesy, a także rozważyć wszystkie okoliczności konkretnej sytuacji. **Tym samym, operator będzie zobowiązany do usunięcia linków jeżeli dostanie istotne i wystarczające dowody, odpowiednie do poparcia żądania usunięcia linków i świadczące o nieprawdziwym charakterze informacji.**

W przypadku nieotrzymania odpowiednich dowodów, operator może odmówić uwzględnienia żądania, aczkolwiek musi liczyć się z ewentualnym odwołaniem się żądającej osoby do sądu lub organu nadzorczego.

Nowe obowiązki operatorów w przypadku otrzymania informacji o postępowaniu

TSUE nałożył na operatorów wyszukiwarki wymóg poinformowania internautów o prowadzeniu postępowania (administracyjnego lub sądowego) w przedmiocie treści, która może okazać się nieprawdziwa, jeżeli dowie się o takim postępowaniu.

Odrębne analizy dotyczące zdjęć

Zgodnie z wyrokiem, **publikację zdjęć w postaci miniatur („thumbnails") należy oceniać w sposób ostrożny, bowiem taka publikacja może stanowić szczególnie poważną ingerencję w prawo do prywatności. W przypadku w którym żądanie usunięcia dotyczy także zdjęć, konieczne jest wykonanie odrębnej analizy (ważenia interesów).** Wartość informacyjna zdjęć powinna być uwzględniania niezależnie od kontekstu ich publikacji na źródłowej stronie internetowej. Powinno ocenić się wszystkie treści bezpośrednio towarzyszące wyświetlaniu zdjęć w wyszukiwarce. Odrębnie należy oceniać sytuację umieszczenia zdjęć jako ilustracji artykułów i opinii oraz sytuację wyświetlania zdjęć poza kontekstem w którym zostały opublikowane na stronie internetowej z której pochodzą.

Wyrok TSUE z dnia 8 grudnia 2022 r.

Zasada rozliczalności – o tym jak mniej nie znaczy więcej w przypadku RODO

Często w kontekście RODO mówi się tworzeniu nadmiernej ilości dokumentacji takich jak klauzule informacyjne, rejestry, polityki bezpieczeństwa itp. Takie działania są uzasadniane **zasadą rozliczalności**. Zgodnie z art. 5 ust. 2 RODO administrator jest odpowiedzialny za przestrzeganie przepisów **i musi być w stanie wykazać ich przestrzeganie**.

W tym kontekście warto wrócić do kary w wysokości 17 milionów euro nałożonej w marcu 2022 r. przez irlandzki organ nadzorczy na Meta Platforms (dawnej Facebook).

Postępowanie w sprawie zostało zainicjowane w wyniku zgłoszenia dwunastu naruszeń ochrony danych osobowych w okresie od 7 czerwca 2018 r. do 4 grudnia 2018 r. W toku postępowania organ badał zgodność z RODO, a w szczególności wdrożenie środków bezpieczeństwa. Ostatecznie decyzja skupiała się nie na ocenie środków bezpieczeństwa, a właśnie realizacji zasady rozliczalności, w kontekście dokumentowania posiadanych środków bezpieczeństwa i sposobu ich wdrożenia. W decyzji nakładającej karę organ wielokrotnie podkreślił, że dokumenty dostarczone przez Meta Platforms w trakcie dochodzenia można uznać za analogiczne do najlepszych praktyk branżowych i stanu wiedzy. Jednak **nie wykazano, aby środki opisane w dokumentacji zostały faktycznie wdrożone w organizacji**.

Główny wniosek płynący z decyzji sprowadza się do tego, że w przypadku przestrzegania RODO nie sprawdza się powiedzenie, że mniej znaczy więcej. **Administrator w ramach zasady rozliczalności nie tylko powinien być w stanie wykazać, że posiada wymagane dokumenty dotyczące przetwarzania danych, ale również być w stanie udowodnić jak procedury opisane w tych dokumentach zostały wdrożone oraz jak w rzeczywistości przebiega ich realizacja.**

Decyzja dostępna jest tutaj

Ciekawe decyzje PUODO w czwartym kwartale 2022 roku

W czwartym kwartale 2022 roku Prezes Urzędu Ochrony Danych Osobowych wydał kilka interesujących decyzji.

1. Decyzja w sprawie P4 sp. z o.o. (Play) – kara za brak odpowiednich środków technicznych oraz organizacyjnych

W dniu 16 listopada 2022 r. PUODO nałożył na spółkę P4 sp. z o.o. – dostawcę usług telekomunikacyjnych marki Play – **administracyjną karę pieniężną w wysokości prawie 1,6 miliona zł** za niewdrożenie przez administratora odpowiednich środków technicznych oraz organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych za pomocą systemów informatycznych służących do rejestracji danych osobowych abonentów usług przedpłaconych, co doprowadziło do uzyskania przez osobę nieuprawnioną dostępu do tych danych.

PUODO ponownie zajmował się tą sprawą (po zaskarżeniu do WSA pierwszej decyzji PUODO w tym przedmiocie sprawa trafiła do ponownego rozpoznania przez PUODO) i po raz kolejny PUODO stwierdził naruszenie przepisów przez administratora.

W tym przypadku, w zgłoszeniu do PUODO naruszania ochrony danych osobowych administrator poinformował o uzyskaniu przez osobę nieuprawnioną dostępu do danych osobowych prawie 115 tysięcy osób (dostęp do rekordów potwierdzeń usług przedpłaconych) w zakresie imienia i nazwiska, numeru PESEL, serii i numeru dowodu osobistego, numeru telefonu, numeru NIP, nazwy podmiotu. Ze względu na zakres ujawnionych danych naruszenie spowodowało wysokie ryzyko naruszenia praw i wolności osób fizycznych.

W ocenie PUODO do naruszenia ochrony danych osobowych abonentów doszło w wyniku wykorzystania podatności systemu informatycznego. Wdrożone przez administratora procedury nie zawierały regulacji dotyczących regularnego testowania, mierzenia i oceniania skuteczności przyjętych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Mimo przyjętych rozwiązań, administrator nie był w stanie wykryć podatności systemu ze względu na brak regularnych testów. W rzeczywistości administrator w ogóle nie podejmował takich działań (ostatni przegląd środków technicznych i organizacyjnych został przeprowadzony u administratora w maju 2018 roku). Zdaniem PUODO brak takich uregulowań przyczynił się do wystąpienia naruszenia danych osobowych.

Decyzja dostępna jest tutaj

2. Decyzja w sprawie P4 sp. z o.o. (Play) – kara za brak zgłoszenia naruszenia oraz brak zawiadomienia

W dniu 3 listopada 2022 r. PUODO nałożył na spółkę P4 sp. z o.o. **administracyjną karę pieniężną w wysokości 250.000,00 zł** za brak zgłoszenia do PUODO naruszenia ochrony danych osobowych w terminie 24 godzin [krótszy termin zgodnie z art. 174a ust. 1 Prawa Telekomunikacyjnego] od wykrycia naruszenia oraz niezawiadomieniu o naruszeniu abonenta, którego dotyczyło naruszenie.

W tym przypadku, naruszenie polegało na automatycznej wysyłce umowy o świadczenie usług telekomunikacyjnych na adres e-mail podany przez klienta (opcja domyślnie zaznaczona w systemie), który jednak ostatecznie okazał się błędny. O pomyłce klient bezzwłocznie poinformował administratora i zażądał jego usunięcia. Podanie adresu e-mail nie było konieczne do zawarcia umowy, miało jedynie na celu wysyłkę umowy. Umowa zawierała m.in. takie dane jak imię i nazwisko, adres zamieszkania, numer PESEL, serię i numer dowodu osobistego oraz numer telefonu. O naruszeniu PUODO dowiedział się z informacji od osoby, do której został wysłany e-mail z umową (osoba ta posiada takie samo nazwisko jak klient, którego dotyczyło naruszenie). Do momentu wszczęcia postępowania przez PUODO administrator nie traktował zaistniałego zdarzenia jako naruszenia ochrony danych.

W ocenie PUODO administrator uzyskał informacje o naruszenie aż dwukrotnie, tj. pierwszy raz w momencieuzyskanie informacji od klienta o błędnie wskazanym adresie e-mail oraz drugi raz wraz z odbiorem wezwania PUODO do złożenia wyjaśnień w sprawie. Administrator nie podjął jednak żadnych działań, nie przeprowadził analizy zdarzenia. Administrator zawiadomił PUODO o naruszeniu ochrony danych dopiero w momencie wszczęcia postępowania przez PUODO oraz po dokonaniu wglądu w akta sprawy (prawie dwa miesiąca później).Administrator nie zawiadomił PUODO o naruszenie w ustawowym terminie, a w konsekwencji nie zawiadomił również abonenta, którego dane wyciekły, o zdarzeniu celem umożliwienia mu podjęcie działań zapobiegawczych.

Zdaniem PUODO administrator nie podjął dostatecznych środków technicznych i organizacyjnych, które umożliwiłyby weryfikację podanych przez klientów adresów e-mail czy dodatkowego zabezpieczenia wysyłanych kopii umów (np. osobno przesyłane hasło dostępowe).

Decyzja dostępna jest tutaj

3. Decyzja w sprawie Wójta Gminy Dobrzyniewo Duże – kara za brak zabezpieczeń w komputerach przenośnych

W dniu 2 listopada 2022 r. PUODO nałożył na Wójta Gminy Dobrzyniewo Duże administracyjną karę pieniężną w wysokości **8.000,00 zł** za przetwarzania danych osobowych w sposób niezapewniający odpowiedniego bezpieczeństwa danych osobowych poprzez brak wdrożenia odpowiednich środków technicznych oraz organizacyjnych, a w konsekwencji brak możliwości wykazania przestrzegania zasady „integralności i poufności", co stanowi o naruszeniu zasady „rozliczalności".

W tym przypadku, przedmiotem naruszenia była kradzież służbowego laptopa wraz ze znajdującymi się w nim dokumentami zawierającymi dane osobowe z mieszkania pracownika Urzędu Gminy. Laptop był zabezpieczony przed nieautoryzowanym dostępem tylko za pomocą hasła, a jego dysk nie został zaszyfrowany.

Administrator pomimo przeprowadzenia analizy ryzyka i ustalenia ryzyka wystąpienia zagrożenia w postaci kradzieży komputera oraz określenia odpowiedniego technicznego środka bezpieczeństwa w postaci szyfrowania dysku twardego komputera – nie zastosował się do wniosków płynących z własnej analizy. W ocenie PUODO świadczy to o braku wdrożenia środków technicznych i organizacyjnych, a tym samym o braku zapewnienia odpowiedniego poziomu bezpieczeństwa.

Istotne jest zatem nie tylko wdrożenie procedur, ale również ich stosowanie przez administratorów.

Decyzja dostępna jest tutaj

Wokół czynników determinujących ryzyko finansowych konsekwencji naruszeń

Zasady wydawania kar - spostrzeżenia Urzędu Ochrony Danych Osobowych

W przypadku stwierdzenia naruszenia ochrony danych, administratorzy i ich doradcy często starają się oszacować ryzyko nałożenia pieniężnej kary administracyjnej. Na bazie publikacji UODO, w tym zawartych w newsletterze UODO dla IOD (nr 10/2022) przedstawiamy naszą interpretację podejścia regulatora:

- Kara pieniężna jest tylko jedną z możliwych decyzji UODO wydawanej wskutek naruszenia (m.in. możliwe jest także upomnienie oraz nałożenie obowiązku dostosowania operacji przetwarzania danych do RODO).

- W przypadku wycieku danych (utraty poufności danych, np. wysłania danych do nieuprawnionego adresata lub zapoznania się z danymi przez osobę nieuprawnioną) ryzyko administracyjnej kary pieniężnej jest wysokie. Potwierdza to praktyka – do tej pory wszystkie kary administracyjne nałożone z przyczyny niewystarczających środków technicznych i organizacyjnych ochrony danych były nakładane w związku z utratą poufności (np. w związku z uzyskaniem dostępu do bazy danych przez osobę trzecią tak jak w przypadku Morele.net lub kradzieżą sprzętu tak jak w przypadku SGGW.

- Jeżeli naruszenie zasad dotyczących bezpieczeństwa danych prowadziło wyłącznie do utraty dostępności (bez utraty poufności; np. działanie oprogramowania ransomware) zachodzi większe prawdopodobieństwo że zostanie wydane upomnienie, zwłaszcza w przypadku wykazania podjęcia działań naprawczych istotnie ograniczających – w ocenie UODO - ryzyko powtórzenia się naruszenia. Należy wskazać, że wszystkie przykłady decyzji w postaci upomnienia wskazane w najnowszym sprawozdaniu UODO (sprawozdanie z działalności w 2021 r.) rzeczywiście dotyczą przełamania zabezpieczeń skutkującego zaszyfrowaniem danych (są to jednostkowe przykłady wybrane przez UODO). Nie można jednak zakładać, że każdy taki przypadek zakończy się tylko upomnieniem, bowiem naruszenia są oceniane indywidualnie.

- W ramach prowadzonych postępowań UODO dąży także do kształtowania praktyk w zakresie zabezpieczania danych. Tym samym, w toku postępowań dotyczących naruszenia bezpieczeństwa danych UODO weryfikuje przede wszystkim poniższe zagadnienia:

  - analizę ryzyka przeprowadzoną przez administratora (w tym jej kompletność i wszechstronność) – przy czym w naszej ocenie istotne jest także faktyczne zaimplementowanie wyników tej analizy w ramach procesów administratora, w tym dobór na jej podstawie odpowiednich zabezpieczeń danych;

  - sposób i częstotliwość weryfikowania stosowanych środków bezpieczeństwa pod kątem ich skuteczności, w szczególności – jak wynika ze sprawozdania UODO z działalności w 2021 r. – w zakresie podatności, błędów oraz ich możliwych skutków dla systemów oraz ich możliwych skutków dla systemów i podjętych działań minimalizujących ryzyko ich wystąpienia;

  - procedury sporządzania kopii zapasowej danych (przy czym powinny być one odpowiednio szczegółowe i powinny zapewniać kontrolę prawidłowości ich sporządzenia oraz skuteczności odtwarzania danych osobowych) oraz ich skuteczność (np. gdy kopie zapasowe są przechowywane z danymi, z których administrator korzysta na bieżąco, mogą być one objęte atakami ransomware, co stoi w sprzeczności z funkcją kopii zapasowych);

  - systemy informatyczne i urządzenia wykorzystywane do przetwarzania danych.

- W przypadkach w których administrator nie zawiadomi osób, których dane dotyczą o naruszeniu, mimo że UODO wystąpiło o takie zawiadomienie, nakładane są co do zasady administracyjne kary pieniężne (oczywiście dotyczy to sytuacji w której administrator jest bierny, a nie sytuacji w której neguje konieczność wykonania zawiadomienia). Jak wskazano w ww. sprawozdaniu, tylko jedna decyzja w 2021 r. dotyczyła nieprzestrzegania nakazu UODO (kara nałożona na przedsiębiorcę prowadzącego działalność z zakresu ochrony zdrowia), przy czym nakaz ten dotyczył właśnie zawiadomienia osób, których dane dotyczą, o naruszeniu.

Nie każde naruszenie przepisów RODO może skutkować odszkodowaniem
Opinia Rzecznika Generalnego TSUE w sprawie C-300/21

W sprawie C-300/21 zawisłej przed TSUE rzecznik generalny Manuel Campos Sánchez-Bordona wydał opinię dotyczącą przesłanek prawa do odszkodowania na gruncie art. 82 RODO.

Zgodnie z art. 82 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Regulacja zawarta w art. 82 RODO stanowi tzw. private enforcement – pozwala, aby każda osoba której dane zostały naruszone mogła samodzielnie dochodzić ochrony sądowej. Odpowiedzialność, o której mowa w art. 82 RODO, dotyczy zarówno szkody majątkowej, jak i niemajątkowej.

Wykładania art. 82 RODO wzbudza jednak wątpliwości co do przesłanek odpowiedzialności przewidzianej w tym przepisie. Jedna z nich dotyczy przesłanki winy. Brzmienie polskiej wersji językowej art. 82 RODO wskazuje, że odpowiedzialność ta opiera się na zasadzie winy (winy objętej domniemaniem, którego obalenie obciąża pozwanego administratora lub podmiotu przetwarzającego). Jednakże porównanie z treścią innych wersji językowych art. 82 RODO przemawia za tym, że przesłanką tej odpowiedzialności nie jest wina. W wersjach obcojęzycznych przyjęto, że administrator czy podmiot przetwarzający może zostać zwolniony od odpowiedzialności, jeżeli udowodni, że nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę („dowód braku odpowiedzialności"). Podnosi się zatem, że odpowiedzialność z art. 82 RODO jest raczej odpowiedzialnością na zasadzie ryzyka.

Sprawa C-300/21 dotyczy skargi jednego z klientów poczty austriackiej Österreichische Post AG, publikującej bazy adresowe, która zbierała informacje na temat sympatii politycznych społeczeństwa austriackiego. Korzystając z algorytmów Österreichische Post AG uznawała ludzi za grupy docelowe dla reklamy wyborczej określonych partii politycznych. Dane te nie były przekazywane osobom trzecim. Działanie Österreichische Post AG wzbudziło oburzenie jednego z klientów, który poczuł się urażony faktem, że Österreichische Post AG uznała go za sympatyzującego z konkretną partią polityczną, co spowodowało u niego wielkie wzburzenie i utratę zaufania, a także poczucie kompromitacji jego osoby.

Nie wyraził on również zgody na przetwarzanie jego danych osobowych w takim celu. Skarżący zażądał 1.000 euro odszkodowania tytułem poniesienia szkody niemajątkowej (wewnętrznego dyskomfortu). Sądy obydwu instancji oddaliły pozew uznając, że naprawieniu podlegają szkody wykraczające poza wzburzenie i stany emocjonalne (zwykłego dyskomfortu czy zwykłego uczucia nieprzyjemności). Sprawa trafiła do austriackiego Sądu Najwyższego, który zwrócił się do TSUE z trzema pytania prejudycjalnymi.

Czy szkoda jest warunkiem koniecznym odszkodowania, czy też wystarczy samo naruszenie RODO?

W ocenie Rzecznika szkoda majątkowa lub niemajątkowa jest warunkiem koniecznym odszkodowania na podstawie art. 82 RODO. Odpowiedź przeciwna, tj. uznanie, że samo naruszenie przepisów RODO skutkuje powstaniem prawa do odszkodowania – niezależnie od faktu powstania szkody – prowadziłaby do uznania na gruncie RODO odpowiedzialności o charakterze karnym. W ocenie Rzecznika nie ma żadnych podstaw do takiej wykładni. RODO w sposób wyraźny rozdziela zakres odpowiedzialności za naruszenia w sferze publicznoprawnej (możliwość nakładania przez organy nadzorcze kar pieniężnych) oraz prywatnoprawnej (możliwość dochodzenia przez podmioty danych odszkodowania). Rzecznik podkreśla również, że wykładnia art. 82 ust. 1 RODO nie daje podstaw do twierdzenie, że istnieje domniemanie szkody w przypadku naruszenia przepisów RODO.

Czy wysokość odszkodowania zależy od innych wymogów prawa UE oprócz zasad skuteczności i równoważności?

Rzecznik wskazał, że zasada skuteczności oraz równoważności nie mają zasadniczego znaczenia, gdyż RODO harmonizuje regulację odszkodowań – art. 82 ust. 1 RODO stanowi niezależną podstawę do stwierdzenia istnienia roszczenia odszkodowawczego. Jednocześnie Rzecznik wskazuje, że obliczanie odszkodowania nie zostało uregulowane w RODO. Rzecznik nie wykluczył możliwości, aby do ustalenia wysokości odszkodowania miały zastosowanie krajowe przepisy.

Czy istotna jest waga samego naruszenia dla stwierdzenia poniesienia szkody niemajątkowej?

Rzecznik stwierdza, że nie każda szkoda niemajątkowa podlega odszkodowaniu. Istotne jest rozróżnienie przypadków naruszenia RODO, w których dochodzi do szkody niemajątkowej podlegającej naprawieniu w drodze odszkodowania od „innych niedogodności" wynikających z nieprzestrzegania przepisów RODO, które ze względu na swój niewielki rozmiar niekonieczne rodziłyby prawo do odszkodowania. W ocenie Rzecznika „złość lub wzburzenie" spowodowane naruszeniem przepisów RODO nie zasługują na odszkodowanie.

Opinia Rzecznika może budzić wątpliwości jako próba ograniczania prawa do odszkodowania za szkody niematerialne. Rzecznik dopuszcza możliwość kreowania przez państwa członkowskie własnych „progów" lub innych przepisów krajowych, które mogą ograniczać wyraźnie przewidziane pełne odszkodowanie za szkody niematerialne na gruncie GDPR. W tym kontekście, orzeczenie TSUE może mieć istotne znaczenie dla praktyki sądów krajowych.

Decyzja dostępna jest tutaj

CIEKAWOSTKI

Plan kontroli sektorowych UODO na 2023 r.

18 stycznia 2023 r. UODO opublikowało plan kontroli sektorowych na 2023 r. W planie tym wskazano, że planowana jest kontrola:

- organów przetwarzających dane osobowe w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym (SIS i VIS) na podstawie przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczpospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, aktów wykonawczych oraz przepisów Unii Europejskiej;

- podmiotów przetwarzających dane osobowe przy użyciu aplikacji mobilnych w zakresie sposobów zabezpieczenia i udostępniania danych osobowych przetwarzanych w związku z użytkowaniem aplikacji;

- podmiotów przetwarzających dane osobowe przy użyciu aplikacji internetowych (webowych) w takim samym zakresie jak kontrola aplikacji mobilnych.

Co ciekawe, dwa pierwsze kontrolowane sektory były już wskazane w planie kontroli na 2022 r. Nie zostało jeszcze opublikowane sprawozdanie z działalności UODO w 2022 r., w którym można byłoby się doszukiwać komentarza UODO związanego z powtórzeniem ww. tematów kontroli.

Istotne jest, że kontrole związane z aplikacjami (mobilnymi i internetowymi) nie są ograniczone do konkretnego rodzaju podmiotów/sektora. Tym samym potencjalnie każdy administrator danych może być objęty kontrolą w tym zakresie. Możliwe także, że UODO zacznie wydawać wytyczne (i decyzje) istotnych tematach związanych z prywatnością w aplikacjach, np. o cookies lub profilowaniu.

AUTORZY:

Agata Szeliga
Partner, radca prawny
agata.szeliga@skslegal.pl
+48 698 660 648

Sylwia Macura-Targosz
Starszy Prawnik, radca prawny
sylwia.macura-targosz@skslegal.pl
+48 694 415 447

Maciej Jakubowski
Prawnik, radca prawny
maciej.jakubowski@skslegal.pl
+48 882 630 942

Jakub Derulski
Prawnik, adwokat
jakub.derulski@skslegal.pl
+48 880 780 275

Katarzyna Wnuk
Prawnik, adwokat
katarzyna.wnuk@skslegal.pl
+48 602 151 178

www.skslegal.pl