

Informujemy, iż w celu optymalizacji treści dostępnych w naszym serwisie i dostosowania ich do Państwa indywidualnych potrzeb korzystamy z informacji zapisanych za pomocą plików cookies na urządzeniach końcowych użytkowników. Pliki cookies użytkownik może kontrolować za pomocą ustawień swojej przeglądarki internetowej. Dalsze korzystanie z naszego serwisu internetowego bez zmiany ustawień przeglądarki internetowej oznacza, iż użytkownik akceptuje stosowanie plików cookies.

[Akceptuję pliki cookies](#)

MENU

[Instrukcja korzystania z BIP](#)

[Nabór](#)

[Zamówienia publiczne](#)

[Organizacja przyjmowania i załatwiania skarg i wniosków](#)

[Podstawa prawna powstania Centrum Usług Informatycznych w Białymstoku](#)

[Plan zamówień publicznych](#)

[Sprawozdania finansowe](#)

[Dostęp do informacji publicznej nieudostępnionej w BIP](#)

[Ochrona danych osobowych](#)

[Cyberbezpieczeństwo](#)

[Zarządzenia](#)

[Petycje](#)

[Sygnałista](#)

[Raport o stanie zapewnienia dostępności podmiotu publicznego
zgłoszeń naruszeń prawa](#)

Zagrożenia związane z niewłaściwym przetwarzaniem danych osobowych.

Najczęstsze naruszenia RODO w 2024r. - wnioski z decyzji PUODO – przed czym należy się bronić?

W XXI w. ochrona danych osobowych stała się jednym z kluczowych zagadnień w życiu prywatnym, jak i zawodowym. Dynamiczny rozwój technologii, digitalizacja usług oraz globalizacja sprawiają, że dane osobowe są gromadzone, przetwarzane i wykorzystywane w sposób coraz bardziej złożony. W Polsce ten temat zyskuje na znaczeniu, zwłaszcza po wejściu w życie w roku 2016 ogólnego rozporządzenia o ochronie danych osobowych (RODO), stosowanego od 2018r., które nałożyło obowiązki na przedsiębiorców, instytucje publiczne oraz inne podmioty przetwarzające dane.

Zagrożenia związane z niewłaściwą ochroną danych osobowych

Choć przepisy prawa oferują szeroką ochronę, w praktyce wciąż istnieją liczne zagrożenia związane z niewłaściwym przetwarzaniem danych osobowych. Należą do nich:

- Ataki hakerskie i cyberprzestępczość (wzrost liczby ataków na systemy komputerowe sprawia, że dane osobowe, takie jak numery PESEL, numery kont bankowych czy dane logowania, stają się łatwym celem, ataki złośliwego oprogramowania - w tym ransomware)
- Zbieranie danych bez zgody (niektóre firmy, aplikacje mobilne czy strony internetowe gromadzą dane użytkowników bez ich pełnej wiedzy i zgody, co stanowi naruszenie prawa)
- Profilowanie i manipulacja (zaawansowane technologie, takie jak AI pozwalają na analizowanie ogromnych zbiorów danych, co prowadzi

do nieetycznych praktyk marketingowych, a także manipulowanie opinią publiczną)

- Nieautoryzowany dostęp do danych:
 - udostępnienie danych osobom trzecim,
 - przetwarzanie danych w celach innych niż pierwotnie określone - samowolna zmiana przez pracownika organizacji celu przetwarzania danych (wysłanie bazy danych osobie trzeciej, poza obszar przetwarzania),
 - upublicznienie dokumentów znajdujących się w porzuconej przesyłce (utrata kontroli nad danymi),
 - zgubienie zewnętrznego nośnika danych (pendrive),
 - wysłanie do nieuprawnionego adresata wiadomości e-mail zawierającej niezabezpieczoną hasłem bazę danych,
 - udostępnienie na profilu mediów społecznościowych listy uczestników określonego przedsięwzięcia.

W 2024 r. Prezes Urzędu Ochrony Danych Osobowych wydał 20 decyzji nakładających administracyjne kary pieniężne na 24 podmioty.

W 2024 r. polskie firmy zapłaciły w sumie 13,9 mln zł kar z tytułu łamania przepisów RODO. Zdecydowaną większość, bo aż 98,7 proc. nałożono na firmy prywatne.

mBank ukarany przez PUODO największą karą: Grzywna na poziomie 4 milionów złotych – nie zawiadomił klientów o wycieku danych!

„Naruszenie polegało na braku zawiadomienia osób poszkodowanych wyciekiem danych, po tym jak dane grupy klientów banku trafiły do innej instytucji finansowej. Bank uznał, że dane trafiły do podmiotu zaufanego, którego obowiązuje tajemnica bankowa, dlatego nie powiadomił osób poszkodowanych, uznając, że zdarzenie nie stwarza dla ich danych wysokiego ryzyka” – argumentacja prawniczkii z kancelarii prawnej Grant Thornton.

UODO nie zgodził się z tą argumentacją mBanku i zauważył, że brak powiadomienia poszkodowanych od razu po zaistniałej sytuacji z

końcem czerwca w 2022 roku, stwarzał ryzyko poważnych konsekwencji. Pracownik firmy przetwarzającej dane osobowe na zlecenie banku, pomylił się i przesłał dokumenty klientów do innej instytucji finansowej. Dokumenty wróciły do banku, ale koperta wcześniej została otwarta. Co sprawia, że wgląd do dokumentów mogły mieć osoby trzecie i nie da się wykluczyć, że z dokumentacją się zapoznaly. W dokumentach były: nazwiska i imiona, imiona rodziców, daty urodzenia, numer rachunku bankowego, adres zamieszkania lub pobytu, numer PESEL, dane dotyczące zarobków i/lub posiadanego majątku, nazwisko rodowe matki, seria i numer dowodu osobistego, inne (informacje dotyczące kredytu i nieruchomości). Kara nałożona na jeden z największych banków w Polsce została określona w kwocie 4,05 mln zł (decyzja DKN.5131.1.2024 z dnia 20 sierpnia 2024 roku). Warto podkreślić, że za tego typu naruszenie maksymalna kara zgodnie z przepisami RODO mogła wynieść nawet 337 mln zł.

Ważny wyrok TSUE! Formy grzecznościowe „Pan i Pani” łamią RODO!

W dniu 9 stycznia 2025 r., w sprawie C-394/23 – Trybunał Sprawiedliwości Unii Europejskiej rozstrzygnął kwestię – czy w celu świadczenia usług (w tym przypadku przewozowych, bo sprawa dotyczyła przejazdu francuską koleją SNCF) – mogą być przez przewoźnika zbierane dane dotyczące płci pasażerów, w celu personalizacji komunikacji z klientami ze względu na płeć. Kluczem do zrozumienia istoty sprawy jest podkreślenie, że SNCF wymagało podania informacji wskazującej na tożsamość płciową, a to po to, żeby zawrzeć i wykonać każdą umowę przewozu koleją. Okazuje się, że przetwarzanie danych dotyczących płci klientów w tym celu – nie może być uznane za niezbędne do wykonania umowy i ponadto może stanowić dyskryminację ze względu na tożsamość płciową.

„Trybunał przypomniał, że zgodnie z zasadą minimalizacji danych, która jest wyrazem zasady proporcjonalności, zbierane dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.”^[1]

Komisja Europejska umożliwiła uczestnikom rejestrację na konferencję „GoGreen” przez Facebooka, co skutkowało karą 400 EURO!

W tym sporze chodzi o działanie przygotowanej przez KE strony internetowej poświęconej przyszłości Europy. Umożliwiała ona zarejestrowanie się do udziału w wydarzeniu „GoGreen”, czyli konferencji poświęconej Zielonemu Ładowi, m.in. poprzez zalogowanie się z użyciem konta użytkownika Facebooka. Z tej opcji skorzystał obywatel Niemiec. Problem w tym, że dane użytkownika, w tym m.in. jego adres IP, Facebook przekazał do USA, gdzie ma swoje serwery. Tymczasem w marcu 2022 r., kiedy obywatel Niemiec rejestrował się na stronie administrowanej przez KE, nie obowiązywała żadna umowa ze Stanami Zjednoczonymi, która uprawniałaby do transferu danych Europejczyków za ocean. Z tego względu obywatel Niemiec zażądał od KE odszkodowania i zadośćuczynienia.^[2] Na podstawie wyroku sądu z dnia 8 stycznia 2025 roku^[3] (Dokument 62022TJ0354), komisja została zobowiązana do zapłaty kwoty 400 EUR na rzecz T.Bindl tytułem zadośćuczynienia za doznaną krzywdę.

Najniższa kara za naruszenie RODO: Wolontariusz ujawnia nadmiarowe dane uczestników zawodów na portalu społecznościowym.

Z kolei najniższą karę Urząd Ochrony Danych Osobowych wymierzył Stowarzyszeniu „Maraton” z Gorlic za brak odpowiedniej reakcji na naruszenie ochrony danych osobowych. – *„Nieprzeszkolony wolontariusz nieopatrznie ujawnił na portalu społecznościowym nadmiarowe dane ponad stu uczestników zawodów sportowych”* – argumentuje prawnik z zespołu kancelarii prawnej w Grant Thornton. Stowarzyszenie zostało ukarane grzywną administracyjną w wysokości 916,71 zł (decyzja DKN 5131.58.2022 z dnia 30 kwietnia 2024 roku). Prezes UODO otrzymał sygnał o incydencie i poprosił o wyjaśnienia. Stowarzyszenie przyznało się do błędu, obwiniając wolontariusza. Organ nadzorczy kilkakrotnie prosił o informacje, ale ich nie otrzymał, więc wszczął postępowanie administracyjne. Stowarzyszenie nie przeprowadziło oceny ryzyka i nie zgłosiło incydentu, co było naruszeniem obowiązków wynikających z RODO.^[4]

Przed czym szczególnie należy się bronić – najczęstsze naruszenia RODO?

Analiza nałożonych kar wskazuje na kilka kluczowych obszarów, w których sektor prywatny/ publiczny powinny szczególnie skoncentrować swoje wysiłki w zakresie ochrony danych osobowych:

- Niezawiadomienie osób o naruszeniu danych: Obowiązek informowania osób, których dane zostały naruszone, jest kluczowy. Niedopełnienie tego obowiązku może prowadzić do poważnych sankcji finansowych.
- Brak odpowiednich zabezpieczeń technicznych i organizacyjnych: Niewystarczające środki ochrony danych osobowych mogą prowadzić do ich wycieku lub nieautoryzowanego dostępu, co skutkuje poważnymi konsekwencjami finansowymi.
- Niewłaściwe przetwarzanie danych osobowych: Naruszenia związane z niezgodnym z prawem przetwarzaniem danych, takie jak brak zgody osoby, której dane dotyczą, czy przetwarzanie danych w celach innych niż pierwotnie określone, są poważnym naruszeniem przepisów RODO.
- Brak współpracy z organami nadzorczymi: Niedostateczna współpraca z organami ochrony danych osobowych, w tym nieudzielanie wymaganych informacji czy nieprzestrzeganie zaleceń, może prowadzić do nałożenia kar.

Środki ochrony:

- Przestrzeganie zasad RODO i innych przepisów prawa o ochronie danych osobowych.
- Regularne aktualizowanie oprogramowania i systemów.
- Stosowanie zapór ogniowych, systemów antywirusowych oraz monitorowania ruchu sieciowego.
- Szyfrowanie danych, stosowanie silnych haseł i dwuetapowej weryfikacji.
- Ograniczenie dostępu do danych na podstawie uprawnień i ich aktualizowanie.
- Zapewnienie szkoleń pracownikom na temat bezpieczeństwa danych.
- Audyty zgodności z regulacjami ochrony danych.

Podsumowując, ochrona danych osobowych jest jednym z fundamentalnych elementów współczesnego społeczeństwa informacyjnego. W Polsce, w kontekście coraz częstszej wymiany danych w sieci, przestrzeganie odpowiednich regulacji, w szczególności takich jak RODO, jest niezbędne do zapewnienia prywatności osób fizycznych oraz ich bezpieczeństwa. Tylko poprzez edukację, odpowiednie zabezpieczenia i świadome zarządzanie danymi, możemy skutecznie chronić się przed zagrożeniami, związanymi z niewłaściwym przetwarzaniem danych osobowych. RODO wciąż rozwija się, a orzecznictwo dotyczące ochrony danych osobowych staje się coraz bardziej obszerne. Dla nas, oznacza to zarówno większe prawa, jak i obowiązki związane z przestrzeganiem przepisów. Warto mieć świadomość, że regulacje te wpływają na nasze codzienne życie, a ich przestrzeganie jest kluczowe dla zapewnienia ochrony naszych danych osobowych.

Niniejsze opracowanie, prezentujące wnioski z decyzji PUODO, ma na celu wskazanie jego czytelnikom, przed czym należy się szczególnie bronić przetwarzając dane osobowe.

Źródło: Gazeta Prawna/ Dziennik Gazeta Prawna; autor Nikodem Chinowski, data wydania 15 luty 2025 14:15

[1] K. Koślicki, TSUE: Tożsamość płciowa klienta nie należy do danych niezbędnych do zakupu biletu, LEX/el. 2025.

[2] <https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/9708191,wyrok-na-komisje-europejska-za-strone-o-zielonym-ladzie-zaplaci-40.html>

[3] <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A62022TJ0354&qid=1739790934559>

[4] <https://biznes.gazetaprawna.pl/artykuly/9739479,4-mln-kary-dla-mbanku-to-rekord-za-lamanie-przepisow-rodo.html>

METRYKA STRONY

REJESTR ZMIAN