Warszawa, 06.02.2025 r.

Raport DLA Piper: Kary za naruszenia RODO i incydenty związane z ochroną danych

Pod koniec stycznia eksperci DLA Piper przedstawili wyniki raportu „GDPR Fines and Data Breach Survey[1]" (Raport dotyczący kar za naruszenia RODO oraz incydentów związanych z danymi) z okazji obchodów Europejskiego Dnia Ochrony Danych. Raport obejmuje 31 krajów europejskich.
To już siódma edycja corocznego raportu DLA Piper, która wybitnie podsumowuje trendy na „rynku ochrony danych osobowych" i wskazuje Administratorom na potencjalne zagrożenia.
W 2024 roku w Europie nałożono łącznie kary na kwotę 1,2 miliarda EUR (1,26 miliarda USD / 996 milionów GBP). Łączna suma kar nałożonych od momentu wprowadzenia RODO w 2018 roku wynosi obecnie 5,88 miliarda EUR (6,17 miliarda USD / 4,88 miliarda GBP). Największa kara kiedykolwiek nałożona na mocy RODO pozostaje kara w wysokości 1,2 miliarda EUR (1,26 miliarda USD / 996 milionów GBP) nałożona przez Irlandzką DPC[2] na Meta Platforms Ireland Limited w 2023 roku.

Trendy i wnioski

W 2024 roku organy nadzoru ochrony danych w Europie kontynuowały intensywne działania w zakresie egzekwowania przepisów RODO, nakładając wysokie kary na podmioty naruszające przepisy o ochronie danych osobowych. Po sześciu latach nakładania kar sięgających setek milionów euro organy te mają teraz silniejszą pozycję i podstawy (w postaci utrzymanych wcześniej kar), na których mogą się opierać.
W 2024 roku organy nadzoru ochrony danych w Europie nałożyły łącznie kary na kwotę 1,2 miliarda EUR (1,26 miliarda USD / 996 milionów GBP). W porównaniu do sumy kar nałożonych w 2023 r. jest to spadek o 33% [w 2023 r. suma nałożony kar wyniosła 1,78 miliarda EUR (1,87 miliarda USD / 1,48 miliarda GBP)].
Spadek ten wynika częściowo z faktu, że dane za 2023 rok zostały zniekształcone przez rekordową karę nałożoną przez irlandzki organ ochrony danych na Meta (1,2 miliarda EUR). W 2024 roku żaden organ nadzorczy nie pobił ani nie zbliżył się do tego rekordu.
Podobnie jak w poprzednich latach, największe kary były nakładane na gigantów technologicznych i firmy z branży mediów społecznościowych – dziewięć z dziesięciu najwyższych kar dotyczyło firm z tego sektora.
W tym roku:

- Irlandzka Komisja Ochrony Danych nałożyła karę w wysokości **310 milionów EUR** (326 milionów USD / 257 milionów GBP) na **LinkedIn** oraz **251 milionów EUR** (264 miliony USD / 208 milionów GBP) na **Meta;**
- Holenderski Urząd Ochrony Danych nałożył karę w wysokości **290 milionów EUR** (305 milionów USD / 241 milionów GBP) na popularną **aplikację do zamawiania przejazdów** w związku z transferem danych osobowych do państwa trzeciego;

Egzekwowanie przepisów w 2024 roku znacząco rozszerzyło się także na inne sektory, w tym usługi finansowe i energetykę:

- Hiszpański Urząd Ochrony Danych nałożył dwie kary o łącznej wysokości **6,2 miliona EUR** (6,5 miliona USD / 5,1 miliona GBP) na **dużą bankową instytucję** za niewystarczające środki bezpieczeństwa;

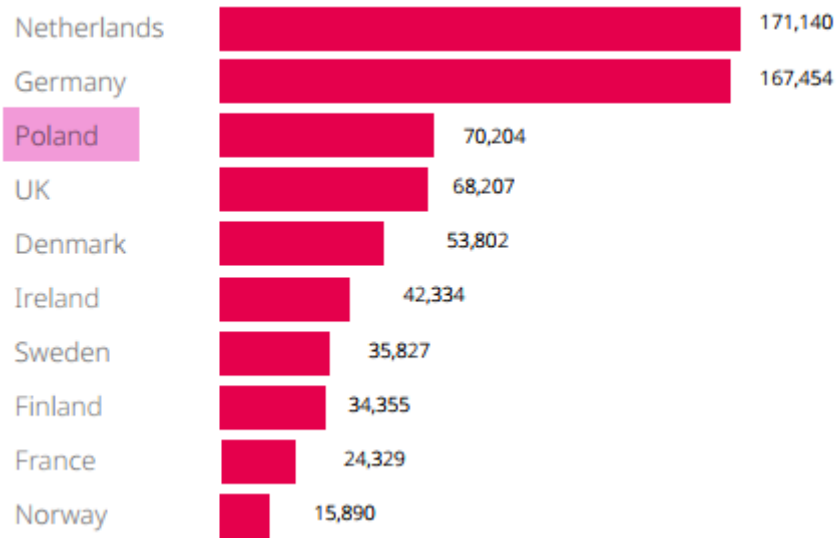
[1] https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024.
[2] The Data Protection Commission.

- Włoski Urząd Ochrony Danych nałożył karę w wysokości **5 milionów EUR** (5,25 miliona USD / 4,15 miliona GBP) na **dostawcę usług używających przestarzałych danych klientów.**

Wielka Brytania stanowiła wyjątek w 2024 roku, nakładając bardzo niewiele kar. Komisarz organu nadzorczego Wielkiej Brytanii, John Edwards, cytowany przez brytyjską prasę w listopadzie 2024 roku[3], powiedział, że nie zgadza się z opinią, iż kary mają największy wpływ na administratorów danych. Wskazał, że procesy odwoławcze od kar mogą trwać latami i pochłaniać cenne zasoby organu nadzorczego. Sukcesywnie wygrane odwołania administratorów lub zmniejszenie wysokości kar mogą osłabić proces egzekwowania i skuteczność odstraszania, a także podważyć pewność i efektywność zespołów zajmujących się dochodzeniami i egzekwowaniem przepisów w organach ochrony danych. Alternatywnym podejściem jest nakładanie mniejszych kar, ale częściej, co preferują władze w krajach, wskazanych powyżej, takich jak Włochy czy Hiszpania.

Liczba zgłoszeń naruszeń danych

Średnia liczba powiadomień o naruszeniach danych na dzień wzrosła nieznacznie do 363 z 335 w ubiegłym roku, co wskazuje na pewną stabilizację liczby zgłoszeń.
Zgodnie z badaniem DLA Piper od czasu wejścia w życie RODO 25 maja 2018 roku do 27 stycznia 2025, nie zaszły większe zmiany w czołówce krajów zgłaszających najwięcej naruszeń do organów nadzorczych - Holandia, Niemcy i Polska pozostają na podium z odpowiednio 33 471, 27 829 i 14 286 zgłoszeniami.



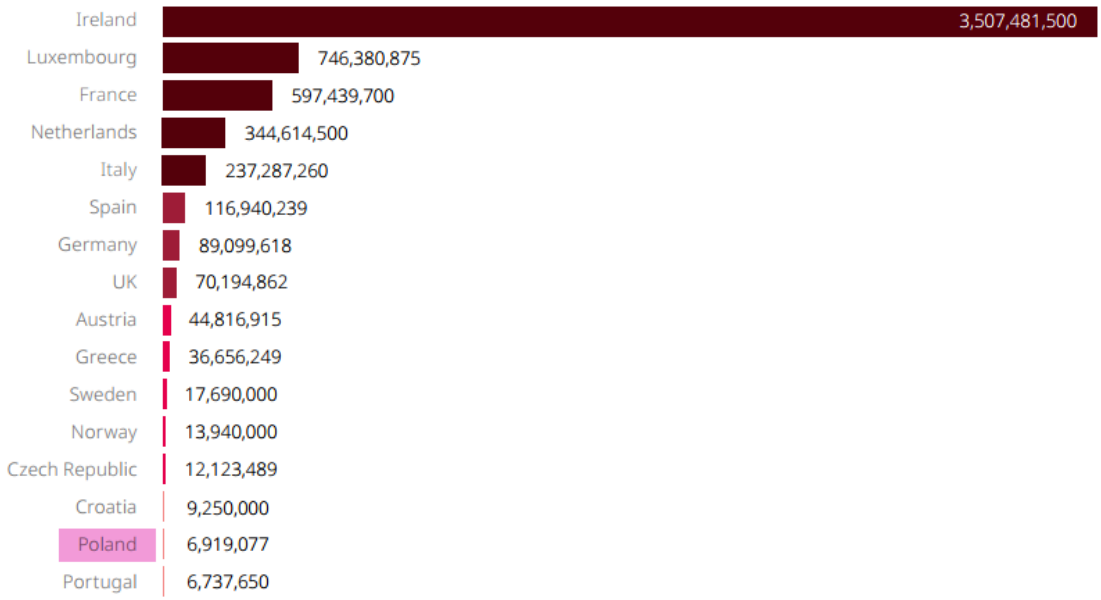
[4] *Top 10 krajów z największą łączna liczba powiadomień o naruszeniu ochrony danych osobowych w okresie od 25 maja 2018 r. do 27 stycznia 2025 r. włącznie.*

Tabela łącznych kar na poziomie krajów

Nie ma zmian na szczycie tabeli krajów pod względem łącznych kar nałożonych do tej pory – Irlandia nadal zajmuje pierwsze miejsce, z karami wynoszącymi obecnie 3,5 miliarda EUR (3,7 miliarda USD / 2,9 miliarda GBP). Irlandzki organ ochrony danych (Irish DPC) nałożył osiem z dziesięciu najwyższych kar do tej pory. Jak przewidywano w ubiegłorocznym raporcie, biorąc pod uwagę popularność Irlandii

[3] https://www.thetimes.com/business-money/companies/article/big-fines-on-tech-companies-are-counter-productive-says-regulator-bfkpc6xrk.
[4] [4] https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024, str. 22.

jako siedziby wielu firm z sektora mediów społecznościowych i technologii opartych na danych, a także fakt, że Irish DPC jest często głównym organem nadzorczym dla przetwarzania danych transgranicznych w całej UE, nie jest zaskoczeniem, że Irlandia utrzymała pierwsze miejsce w tabeli kar nałożonych w tym roku.
Luksemburg nadal zajmuje drugie miejsce w tabeli krajów z łącznymi karami wynoszącymi 746,38 miliona EUR (784 miliony USD / 619 milionów GBP), głównie z powodu dużej kary nałożonej w 2021 roku na amerykańskiego detalistę internetowego i platformę e-commerce (kara wynosząca 746 milionów EUR, która nadal jest przedmiotem odwołania).



[5] *Łączna wartość kar nałożonych na mocy RODO od 25 maja 2018 r. do 27.01.2025 r. (w euro)*

Kluczowa decyzja – Clearview AI

Ciekawe aspekty ochrony danych osobowych zostały poruszone w jednej z ostatnich decyzji holenderskiego organu ochrony danych. We wrześniu 2024 roku holenderski organ (Dutch DPA) nałożył karę w wysokości 30,5 miliona EUR (32,03 miliona USD / 25,32 miliona GBP) na dostawcę oprogramowania do rozpoznawania twarzy, firmę Clearview AI.
Clearview AI zbierała obrazy twarzy ludzi oraz dane z publicznie dostępnych informacji w Internecie i na platformach mediów społecznościowych na całym świecie, tworząc globalną bazę danych do rozpoznawania twarzy. Osoby, których dane były wykorzystywane w ten sposób, nie były o tym informowane, a sama baza zawierała ogromną ilość danych.
Po serii skarg, które miały miejsce od maja 2021 roku, zgłoszonych przez aktywistów ochrony prywatności, kilka organów nadzorczych nałożyło kary finansowe na Clearview AI za naruszenia RODO. Pomimo tych kar, Clearview AI kontynuowało swoje działania w ten sam sposób. W związku z tym holenderski organ ochrony danych zdecydował o nałożeniu dodatkowych kar w wysokości do 5,1 miliona EUR (5,4 miliona USD / 4,2 miliona GBP) za dalsze niezgodności, wskazując, że firma nie zaprzestała naruszeń po zakończeniu postępowania. Co więcej, organ stwierdził, że prowadzi dochodzenie w celu ustalenia, czy może „**pociągnąć do odpowiedzialności osobiście kierownictwo**

[5] https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024, str. 20.

firmy i nałożyć na nie karę za odpowiedzialność za naruszenia[6]”. Holenderski DPA wyjaśnił, że „taka odpowiedzialność istnieje już w przypadku, gdy dyrektorzy wiedzą, że postanowienia RODO są naruszane, mają władzę i narzędzia, by temu zapobiec, ale tego nie robią, świadomie akceptując te naruszenia”.
Tym samym wskazano na możliwą zmianę podejścia ze strony europejskich organów ochrony danych, które mogą zacząć pociągać do odpowiedzialności osobistej członków zarządu za niedopełnienie obowiązków związanych z przestrzeganiem wymagań RODO.

Podsumowanie

Choć w 2024 roku nie odnotowano rekordowych kar, nie świadczy to o zmniejszonym zainteresowaniu egzekwowaniem przepisów RODO.
Zwiększenie nadzoru nad nowymi sektorami, wyższa liczba zgłoszeń naruszeń oraz większa kontrola nad sztuczną inteligencją pokazują, że ochrona danych w Europie pozostaje jednym z głównych priorytetów organów regulacyjnych. Możemy spodziewać się, że 2025 rok przyniesie jeszcze więcej zmian, w tym możliwą odpowiedzialność osobistą dyrektorów/menadżerów za naruszenia RODO (na co wskazuje postępowanie holenderskiego organu wobec Clearview AI).

Nina Zacharska - specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.

[6] https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition.