Analiza wyroków ws. naruszeń RODO

Wnioski dla Twojej firmy

W TYM WYDANIU:

LexDigital

lexdigital.pl

Aleksander Markiewicz
Legal Counsel

Przetwarzanie danych w związku z przyszłymi roszczeniami

analiza wyroku Naczelnego Sądu Administracyjnego

NSA wyrokiem z dnia 8 stycznia 2025 r. (III OSK 4868/21) oddalił skargę kasacyjną banku Millennium od wyroku WSA w Warszawie (II SA/Wa 607/20), podtrzymując tym samym decyzję Prezesa Urzędu Ochrony Danych Osobowych. Co znaczy ten wyrok i dlaczego jest istotny dla Twojej firmy?

Stan faktyczny i uzasadnienie

Stan faktyczny obejmował przypadek przetwarzania danych osobowych klientów, którzy rozwiązali umowę z bankiem a następnie złożyli sprzeciw dot. przetwarzania ich danych osobowych w celach marketingowych.

Bank wskazał, że dane klientów przetwarzane są w oparciu o uzasadniony interes administratora polegający na konieczności zabezpieczenia potencjalnych roszczeń.

Organ nadzorczy wskazał, że przetwarzanie danych na zapas w celu zabezpieczenia przed roszczeniami, które nie istnieją w chwili rozwiązania stosunku prawnego i są czysto hipotetyczne, jest niedopuszczalne.

W omawianej sprawie zakres danych przetwarzanych w związku z potencjalnymi roszczeniami był bardzo szeroki i zawierał:

- daty i miejsca urodzenia
- obywatelstwo
- imiona rodziców
- stan cywilny
- nazwisko panieńskie matki
- płeć
- adresy zamieszkania i korespondencyjny
- numer telefonu komórkowego

Bank w toku postępowania nie wykazywał również aby dane klientów były przetwarzane w innych celach i w oparciu o inne podstawy prawne.

NSA w uzasadnieniu wskazał, że zgodnie z zasadą rozliczalności (art. 5 ust. 2 RODO) to na administratorze danych spoczywa obowiązek wykazania, że zarówno zakres, jak i sposób przetwarzania danych osobowych jest adekwatny do obranego przez niego celu i warunków jego realizacji

– mówi o tym zasada ograniczonego celu przetwarzania (art. 5 ust. 1 lit. b RODO) i zasady minimalizacji przetwarzania danych (art. 5 ust. 1 lit. c RODO).

Ponadto NSA wskazał, że zastosowanie podstawy z art. 6 ust. 1 lit. f RODO jest uzasadnione, gdy łącznie spełnione są następujące przesłanki:

1. **Po stronie administratora istnieją cele, dla osiągnięcia których przetwarzanie danych osobowych jest niezbędne;**
2. **Cele te wynikają z "prawnie uzasadnionych interesów" realizowanych przez administratora;**
3. **"Prawnie uzasadnione interesy" realizowane przez administratora mają charakter nadrzędny wobec interesów lub podstawowych praw i wolności osoby, której dotyczą przetwarzane dane.**

Zgodnie z uzasadnieniem wyroku – ustalenie "niezbędności" przetwarzania danych osobowych dla celów administratora musi opierać się na przesłankach konkretnych, uwzględniających możliwie najszersze spektrum uwarunkowań jego realizacji. Przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. f RODO wymaga od administratora wykazania, że jest to konieczne z uwagi na charakter celu, okoliczności faktyczne i prawne jego realizacji oraz relacje podmiotowe pomiędzy administratorem a osobą, której te dane dotyczą. Zgodnie z zasadą rozliczalności (art. 5 ust. 2 RODO) administrator będzie zobowiązany wykazać, że zarówno zakres, jak i sposób przetwarzania danych osobowych jest adekwatny do obranego przez niego celu i warunków jego realizacji – patrz: zasada ograniczonego celu przetwarzania (art. 5 ust. 1 lit. b RODO) i zasada minimalizacji przetwarzanych danych (art. 5 ust. 1 lit. c RODO).

Co dalej?

Powyższe, wraz z komunikatem na stronie UODO wskazują, że **nie ma podstaw** do przetwarzania danych w oparciu o uzasadniony interes administratora dla celu obrony i dochodzenia potencjalnych roszczeń.

Jednakże stan faktyczny, w oparciu o który został wydany wyrok może wskazywać, że dotyczy on zakresu możliwych do przetwarzania danych w celu obrony i dochodzenia roszczeń – czyli zasady minimalizacji przetwarzania danych, a nie surowego zakazu przetwarzania danych dla celu obrony i dochodzenia roszczeń.

Niestety taki wniosek nie został wprost sformułowany w wyroku, jednakże z prawnego i biznesowego punktu widzenia brak możliwości przetwarzania określonych danych przez okres przedawnienia roszczeń może w znaczący sposób ograniczać możliwość obrony i dochodzenia roszczeń przez Administratora.

W związku z powyższym należy uznać, że przetwarzanie danych dla obrony przed roszczeniami jest dopuszczalne, ale wymaga dokładnej weryfikacji zakresu i niezbędności przetwarzanych danych.

Ryzyka dla administratora

Omawiane orzeczenie rodzi po stronie administratorów następujące ryzyka:

- **Ograniczenie możliwości obrony banku**

  Orzeczenie to może utrudnić bankom skuteczną obronę przed potencjalnymi roszczeniami klientów, nawet jeśli roszczenia te są nieuzasadnione. Bank, nie mogąc przechowywać danych "na zapas", może mieć trudności w udowodnieniu swojej racji w przypadku sporu.

- **Niepewność prawa**

  Orzeczenie to może wprowadzać niepewność prawa w zakresie przetwarzania danych osobowych przez banki. Banki mogą mieć trudności w określeniu, jakie dane mogą przetwarzać, a jakie nie, co może prowadzić do niepotrzebnego ograniczenia ich działalności.

- **Brak elastyczności**

  Orzeczenie to może być zbyt sztywne i nie uwzględniać specyfiki działalności bankowej. Banki często muszą przetwarzać duże ilości danych, aby zapewnić bezpieczeństwo transakcji i zapobiegać praniu pieniędzy. Orzeczenie to może utrudnić im realizację tych celów.

- **Potencjalne negatywne konsekwencje dla klientów**

  Orzeczenie to może mieć negatywne konsekwencje dla klientów, np. w postaci wydłużonego czasu rozpatrywania reklamacji lub trudności w uzyskaniu kredytu.

Należy jednak zaznaczyć, że orzeczenie NSA z dnia 8 stycznia 2025 r. (III OSK 4868/21) jest **prawomocne i wiążące.**

Sprzeczność z poprzednim wyrokiem w zakresie retencji

Co więcej, omawiany wyrok stoi w sprzeczności z wyrokiem Naczelnego Sądu Administracyjnego z dnia 20 lutego 2024 r. (Sygn. **III OSK 2700/22), w którym NSA wskazał**, że przetwarzanie danych osobowych kandydatów do pracy, którzy nie zostali zatrudnieni jest dozwolone, przez czas przedawnienia potencjalnych roszczeń związanych z procesem rekrutacji, czyli przez maksymalnie 3 lata.

Ponadto NSA wskazał, że przetwarzanie danych osobowych musi być oparte o trzy zasadnicze przesłanki:

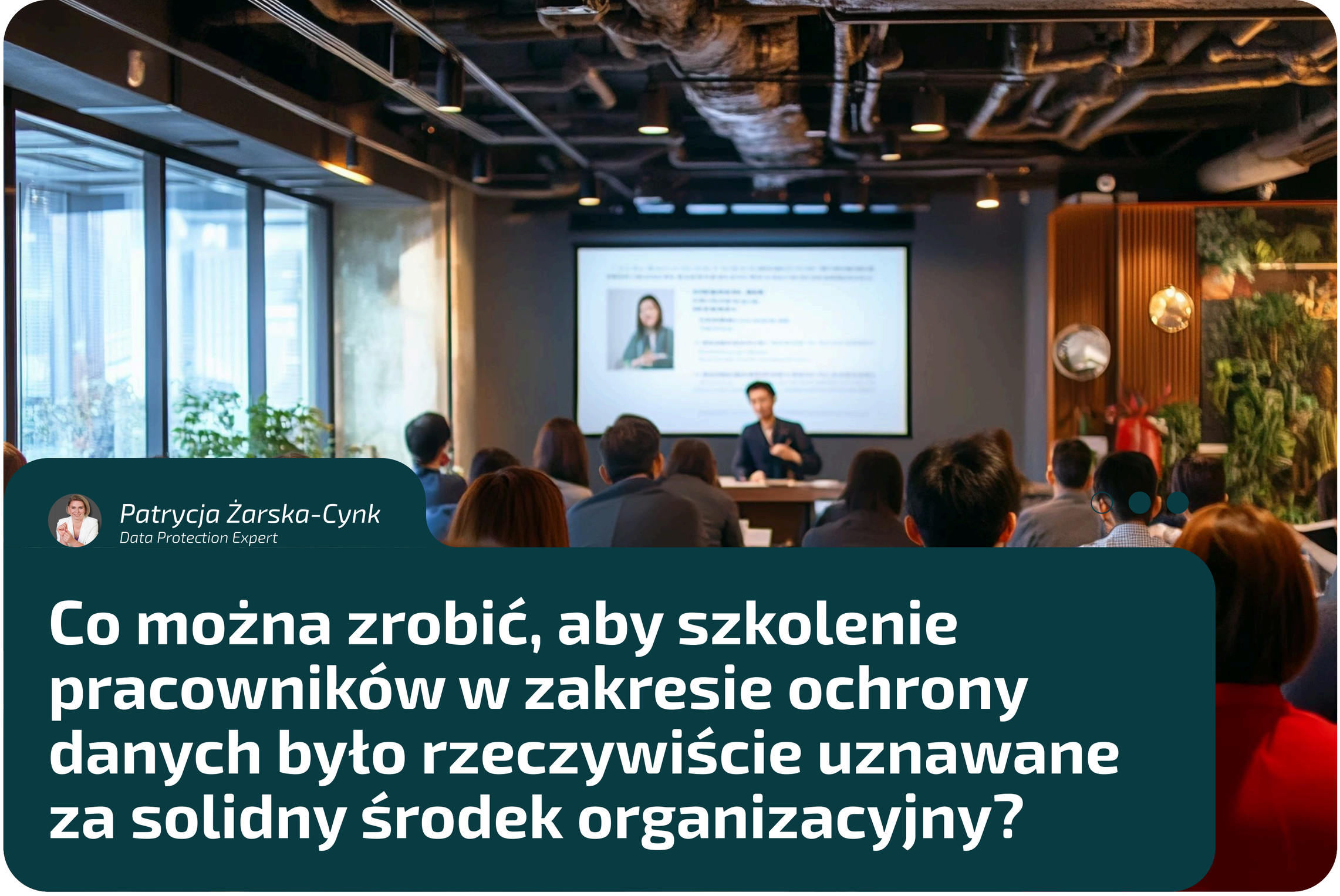
- administrator musi wykazać cele, do których osiągnięcia przetwarzanie danych jest niezbędne
- cele te są uzasadnione interesem prawnym administratora danych
- interes prawny administratora ma charakter nadrzędny w stosunku do praw i wolności osoby której dane są przetwarzane

Podsumowanie

Wyrok NSA z dnia 8 stycznia 2025 r. wskazuje, że administrator nie ma podstaw do przetwarzania danych w oparciu o uzasadniony interes administratora dla celu obrony i dochodzenia potencjalnych roszczeń.

Takie podejście po stronie administratora rodzi wysokie ryzyko związane z brakiem możliwości obrony przed potencjalnymi roszczeniami lub dochodzenia potencjalnych roszczeń.

Przetwarzanie w powyższym celu i w oparciu o uzasadniony interes administratora należy uznać za dopuszczalne, pod warunkiem spełnienia wyżej opisanych kryteriów.



Patrycja Żarska-Cynk
Data Protection Expert

Co można zrobić, aby szkolenie pracowników w zakresie ochrony danych było rzeczywiście uznawane za solidny środek organizacyjny?

Inspiracją do tego artykułu jest decyzja hiszpańskiego organu ochrony danych osobowych (AEPD) oddalająca apelację The Phone House dotyczącą kary za naruszenie RODO. Zarządy firm często dążą do minimalizacji działań związanych z ochroną danych, a szkolenia personelu są jednymi z pierwszych elementów, które podlegają ograniczeniom. Czy słusznie?

Historia The Phone House – co poszło nie tak?

W kwietniu 2021 roku firma The Phone House Spain padła ofiarą ataku ransomware (Babuk Locker), w wyniku którego skradziono dane 13 milionów osób, a następnie opublikowano je w dark webie. Dane obejmowały m.in. imiona i nazwiska, numery identyfikacyjne, adresy, e-maile, numery telefonów, dane bankowe i informacje o urządzeniach.

Naruszenia RODO zidentyfikowane przez AEPD:

1. **Naruszenie zasady integralności i poufności** (art. 5(1)(f) RODO) – niewystarczające zabezpieczenia danych.
2. **Naruszenie obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych** (art. 32 RODO)

AEPD wykazała, że The Phone House:

- nie wdrożyła skutecznych polityk zarządzania hasłami
- nie miała wystarczających zabezpieczeń sieciowych
- nie prowadziła regularnych audytów bezpieczeństwa
- stosowała przestarzałe algorytmy szyfrujące
- ignorowała wcześniejsze zalecenia dotyczące poprawy zabezpieczeń

Przedstawmy zarzuty AEPD wobec The Phone House obrazowo:

Problemy z ochroną danych:

Słabe zarządzanie hasłami

Brak skutecznych zasad dotyczących haseł umożliwił nieautoryzowany dostęp

Niewystarczające szyfrowanie danych

Dane przechowywane w postaci niezaszyfrowanej lub z użyciem przestarzałych algorytmów

Słaba konfiguracja bezpieczeństwa sieciowego

Niewystarczająca ochrona obwodowa i brak monitorowania

Brak regularnych audytów

Brak regularnych kontroli systemów bezpieczeństwa mimo wcześniejszych zaleceń

Brak pseudominizacji

Dane osobowe przechowywane w formach umożliwiających identyfikację zwiększyły ryzyko wycieku

Niewystarczające szkolenia dla pracowników

Brak szkoleń przyczynił się do błędów ludzkich w ochronie danych.

Niewystarczające procedury reagowania na incydenty

Brak skutecznych mechanizmów wykrywania i łagodzenia ataków ransomware.

Konsekwencje dla The Phone House

Za te uchybienia AEPD nałożyła karę w wysokości 6,5 miliona euro, na którą składało się:

- **4 miliony euro** za naruszenie zasady integralności i poufności (art. 5(1)(f)),
- **2,5 miliona euro** za niewdrożenie odpowiednich środków organizacyjnych i technicznych (art. 32).

Firma próbowała odwołać się od tej decyzji, argumentując, że była ofiarą zaawansowanego cyberataku i nawet najlepsze środki ochrony mogłyby nie zapobiec incydentowi. AEPD jednak odrzuciła apelację, wskazując, że obowiązkiem administratora danych jest **proaktywne wdrażanie zabezpieczeń adekwatnych do poziomu ryzyka.**

Stanowisko organów ochrony danych: szkolenia jako fundament zgodności z RODO

Organy ochrony danych osobowych w Europie, takie jak Europejska Rada Ochrony Danych (EDPB), hiszpańska AEPD oraz brytyjski ICO podkreślają kluczową rolę szkoleń personelu w zakresie ochrony danych osobowych. Zarówno w rekomendacjach, jak

i decyzjach, wskazują na obowiązek zapewnienia odpowiednich szkoleń jako istotnego elementu zgodności z RODO.

Stanowiska organów ochrony danych osobowych

Europejska Rada Ochrony Danych (EDPB) w swoich wytycznych dotyczących ochrony danych w fazie projektowania i domyślnie (Privacy by Design and Default) wskazuje, że szkolenia personelu są jednym z podstawowych środków organizacyjnych wymaganych do zapewnienia zgodności z RODO. Szkolenia powinny obejmować zarówno podstawowe zasady ochrony danych, jak i specyficzne zagrożenia związane z przetwarzaniem danych. EDPB podkreśla również konieczność regularnego powtarzania szkoleń, szczególnie w kontekście zmieniających się zagrożeń, takich jak cyberataki.

Hiszpański organ ochrony danych (AEPD), który zainspirował ten artykuł zaleca szkolenie pracowników w zakresie przetwarzania danych osobowych jako część polityki bezpieczeństwa informacji. W szczególności dotyczy to sytuacji pracy zdalnej i mobilnej, gdzie pracownicy muszą być świadomi zagrożeń oraz konsekwencji naruszeń dla osób, których dane dotyczą.

Brytyjski ICO uznaje szkolenia za kluczowy element programu zgodności z przepisami o ochronie danych osobowych i zaleca ich przeprowadzanie na różnych etapach: podczas wdrażania nowych pracowników (induction training), regularnie (refreshers) oraz w razie zmian w przepisach lub procedurach. ICO stwierdziło również, że organizacje, które mogą udokumentować szkolenia dla co najmniej 80% personelu, są mniej narażone na kary finansowe w przypadku naruszeń.

Temat szkoleń w decyzjach organów

Rumunia:

Bank został ukarany grzywną 100 000 euro za bezprawne ujawnienie danych osobowych, co wynikało m.in. z niewystarczającego przeszkolenia personelu.

Bułgaria:

Sąd administracyjny stwierdził naruszenie firmy kurierskiej polegające na braku odpowiednich szkoleń, co doprowadziło do ujawnienia danych klientów nieuprawnionym osobom.

Polska:

W jednej z decyzji Prezesa UODO podkreślono znaczenie szkoleń personelu w kontekście naruszeń ochrony danych. Wskazano, że brak odpowiednich szkoleń może prowadzić do nieprawidłowego przetwarzania danych, co w konsekwencji może skutkować naruszeniem przepisów RODO.

Hiszpania:

Klub piłkarski Real Madryt uniknął kary za naruszenie ochrony danych dzięki wdrożeniu skutecznych środków organizacyjnych, w tym szkoleń personelu w zakresie przetwarzania danych osobowych.

Jakie są konsekwencje braku odpowiednich szkoleń w zakresie ochrony danych osobowych?

Grzywny

Brak szkoleń prowadzi do finansowych kar za naruszenia ochrony danych.

Utrata zaufania

Organizacje zaniedbujące bezpieczeństwo danych ryzykują utratę klientów i kontrahentów w razie incydentu.

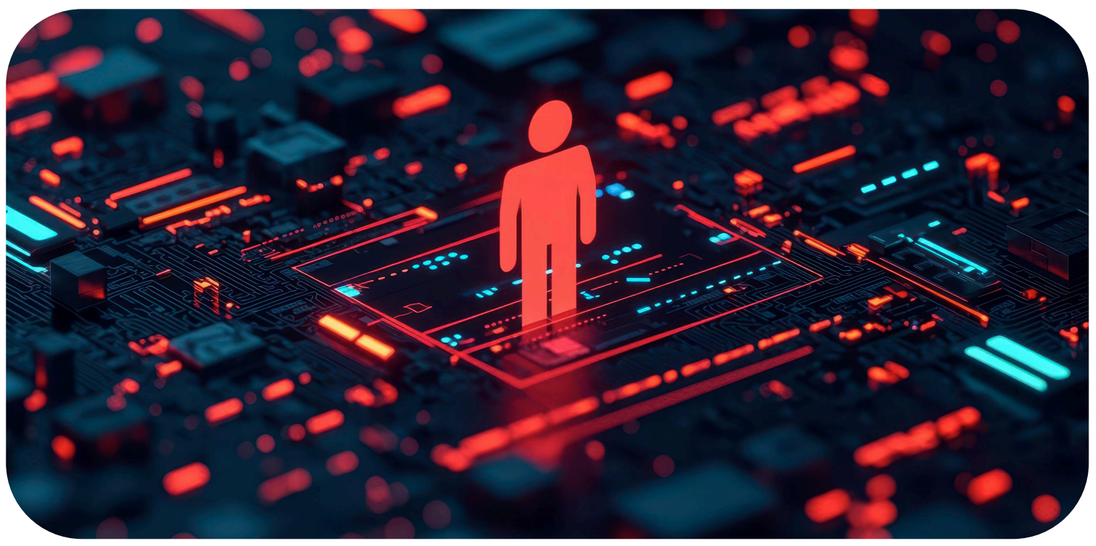
Naruszenia prawne

Niedostateczne szkolenie skutkuje niezgodnymi z prawem ujawnieniami danych.

Jak zapewnić, by szkolenia były solidnym środkiem organizacyjnym?

Badania przeprowadzone pod patronatem UODO wykazały, że 81% firm z sektora MŚP szkoli swoich pracowników z zakresu ochrony danych osobowych, jednak 59% z nich robi to tylko raz – podczas wdrożenia do pracy. Aż 20% przedsiębiorstw nie prowadzi takich szkoleń wcale. UODO zwraca uwagę na konieczność regularnych i cyklicznych szkoleń, dostosowanych do pojawiających się nowych zagrożeń.

Warto zatem zadać sobie pytanie – **czy nasze szkolenia rzeczywiście stanowią skuteczny środek organizacyjny?**



1. **Szkolenie powinno być dostosowane do rzeczywistości biznesowej**

   Unikajmy ogólników i prawniczej retoryki. Zamiast tego koncentrujmy się na realnych zagrożeniach, z którymi pracownicy mogą się spotkać. Szkolenia powinny być dostosowane do specyfiki różnych grup pracowników, np. działu IT, marketingu czy obsługi klienta.

2. **Dokumentacja uczestnictwa**

   Należy rejestrować daty szkoleń, listy uczestników oraz metody uczestnictwa.
   W przypadku szkoleń online warto zachować dane logowania, np. adresy IP uczestników.
   W szkoleniach stacjonarnych można stosować listy obecności lub podpisy.

3. **Szkolenie powinno być obowiązkowe**

   Szkolenia z ochrony danych osobowych nie powinny być opcjonalne. Firmy powinny wprowadzić mechanizmy egzekwowania obowiązku szkoleniowego, a w przypadku odmowy udziału – wdrażać odpowiednie sankcje, np. ostrzeżenia lub ograniczenie dostępu do niektórych systemów.

4 Egzamin końcowy jako dowód skuteczności szkolenia

Warto wdrożyć testy wiedzy na zakończenie każdego szkolenia. Pomagają one zweryfikować poziom zrozumienia zagadnień przez pracowników i stanowią dodatkowy dowód na wdrożenie skutecznych środków organizacyjnych.

5 Regularne odnawianie szkoleń

Szkolenie raz na kilka lat to zdecydowanie za mało. Powinno się je powtarzać co najmniej raz w roku, a w razie potrzeby także po incydentach związanych z ochroną danych. Regularne szkolenia pomagają utrzymać wysoki poziom świadomości w organizacji.

Sekwencja wdrożenia programu szkoleń w organizacji w formie grafiki:

Wnioski – dlaczego szkolenia są kluczowe dla ochrony danych?

Organy ochrony danych w UE jednoznacznie wskazują na konieczność i znaczenie szkoleń personelu w zakresie ochrony danych osobowych jako kluczowego elementu zapewnienia zgodności z RODO i budowania kultury bezpieczeństwa w organizacji. Szkolenia z zakresu ochrony danych osobowych są nie tylko środkiem zapewniającym zgodność z przepisami, ale także kluczowym elementem budowania świadomości wśród pracowników. Przeszkolony personel jest bardziej świadomy potencjalnych zagrożeń i potrafi skuteczniej reagować na incydenty związane z ochroną danych. Regularne i dostosowane do specyfiki organizacji szkolenia minimalizują ryzyko naruszeń i potencjalnych kar finansowych.

Mimo to szkolenia są jednym z **najczęściej pomijanych środków organizacyjnych**, choć mają kluczowe znaczenie dla bezpieczeństwa danych. Brak wiedzy i świadomości wśród pracowników może prowadzić do błędów, które skutkują poważnymi naruszeniami RODO i wysokimi karami finansowymi.

Warto więc spojrzeć na szkolenia nie jako przykry obowiązek, ale jako **strategiczne narzędzie zarządzania ryzykiem**. Inspektor Ochrony Danych (IOD) może odegrać tu kluczową rolę, pomagając firmie opracować **długofalowy plan szkoleń** i monitorować jego skuteczność.

Pamiętajmy, że dobre szkolenia to nie tylko zgodność z RODO – to także **budowanie kultury bezpieczeństwa w organizacji**, która minimalizuje ryzyko incydentów i zapewnia większą ochronę zarówno firmie, jak i jej klientom.

Źródła:

1. AEPD (Spain) - EXP202210465 - GDPRhub
   https://gdprhub.eu/index.php?title=AEPD_%28Spain%29_-_EXP202210465
2. AEPD (Spain) - EXP202305587 - GDPRhub
   https://gdprhub.eu/index.php?title=AEPD_%28Spain%29_-_EXP202305587
3. AEPD (Spain) - EXP202306260 - GDPRhub
   https://gdprhub.eu/index.php?title=AEPD_%28Spain%29_-_EXP202306260
4. Spain | Jurisdictions - DataGuidance
   https://www.dataguidance.com/jurisdiction/spain
5. AEPD impose a fine to a telephone company for a loss of ...
   https://www.edpb.europa.eu/news/national-news/2021/aepd-impose-fine-telephone-company-loss-confidentiality-and-lack-adequate_en
6. GDPR Employee Training | GDPR Compliance | Data Protection
   https://secureprivacy.ai/blog/employee-training-for-gdpr-compliance
7. [PDF] Recommendations to protect personal data in situations of mobility ...
   https://www.aepd.es/guides/recommendations-to-protect-personal-data-situations-mobility-and-telecommuting.pdf
8. Nationwide Tailored GDPR Training Courses for Employees
   https://www.privacyhelper.co.uk/gdpr-training-courses/
9. [PDF] Guidelines 4/2019 on Article 25 Data Protection by Design and by ...
   https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
10. Guidelines, Recommendations, Best Practices
    https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en
11. The Importance of Training Employees on Personal Data Protection
    https://pdtn.org/employee-training-on-personal-data-protection/
12. How to focus data protection training on specific teams
    https://dpnetwork.org.uk/how-to-focus-data-protection-training/
13. *https://uodo.gov.pl/decyzje/DKN.5131.6.2024?utm_source=chatgpt.com*
14. *https://uodo.gov.pl/pl/138/3395?utm_source=chatgpt.com*

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI