RODO promocja się skończyła: trzy ważne orzeczenia i ich konsekwencje

Data 25 maja 2018 roku, to dzień, od którego przepisy RODO zaczęły funkcjonować w praktyce. Na początku Prezes Urzędu Ochrony Danych Osobowych (dalej: UODO) podchodził do naruszeń dość liberalnie. Na pierwszą karę w kwocie 943 tys. zł czekaliśmy w Polsce 10 miesięcy. UODO podobnie jak większość innych europejskich regulatorów, na początku postawił przede wszystkim na edukację. Wszystko wskazuje jednak na to, że wchodzimy właśnie w nowy etap stosowania RODO w praktyce. Na zmianę wskazują trzy bardzo jednoznaczne decyzje, już nie tylko UODO, ale również WSA.

Prawo w akcji

RODO jest ogólnym aktem prawnym, w wielu obszarach podlegającym różnym interpretacjom. Do momentu wydania decyzji administracyjnych czy orzeczeń sądowych, trudno przewidzieć jednoznacznie, w którym kierunku pójdzie praktyka.

W mojej opinii, praktyka jest najcenniejszym źródłem informacji dla każdego Administratora Danych czy IOD. Pozwala przejść ze sfery dywagacji i dyskutowania o RODO, do strefy gdzie RODO naprawdę „się dzieje".

Z jednej strony, decyzje sądów i UODO mogą trochę przytłaczać. Mogą budzić sprzeciw, bo nie zawsze się z nimi zgodzimy. Być może UODO przyjął inną interpretację niż ta, która do tej pory była podstawą naszego działania. Kary są coraz wyższe i jest ich coraz więcej.

Z drugiej strony, uważna lektura uzasadnień decyzji, może być czymś co pozwoli nam uniknąć kary w przyszłości. Daje nam ważny punkt odniesienia. Jeśli pełnimy funkcję IOD, możemy pokazać co dokładnie się może wydarzyć, jeśli rekomendowane przez nas rozwiązanie nie zostanie wdrożone.

Wybrałem dla Ciebie trzy, w mojej opinii, najważniejsze decyzje i dotyczące ich orzeczenia, z którymi warto się zapoznać.

Aleksandrów Kujawski – pierwsi w trzech konkurencjach!

Kara nałożona na Burmistrza Aleksandrowa Kujawskiego jest pierwsza w aż trzech aspektach. To pierwsza kara nałożona na jednostkę administracji publicznej. Zgodnie z polską modyfikacją RODO, jednostki publiczne można ukarać maksymalnie do kwoty 100 tys. zł. Aleksandrów Łódzki ukarano kwotą 40 tys. zł, a więc relatywnie wysoką. To aż 40% górnego ustawowego limitu.

Burmistrz Aleksandrowa Kujawskiego jest także pierwszym Administratorem Danych w Polsce, ukaranym za brak umowy powierzenia! I to pomimo tego, że nie był on stroną umowy głównej. To bardzo istotny sygnał do wszystkich organizacji, które wciąż odwlekają podpisanie swoich umów powierzenia. To również jasny sygnał dla podmiotów pozostających w grupie kapitałowej. Spółka matka może być stroną

umowy głównej, ale jej spółki córki muszą dopilnować tego, aby warunki powierzenia danych zostały zachowane.

I na koniec, decyzja względem Aleksandrowa Kujawskiego to pierwsza kara UODO, która wybroniła się przed Wojewódzkim Sądem Administracyjnym.

Nieco więcej informacji o ww. karze znajdziesz w naszym rejestrze kar UODO.

Morele.net – najwyższa kara zostaje

O decyzji w tej sprawie napisano bardzo dużo. Wysoka kwota kary przyciągnęła uwagę mediów, nie tylko branżowych. My również szczegółowo opisaliśmy ten przypadek na naszym blogu. W telegraficznym skrócie – UODO nałożył karę w kwocie 2 830 410 zł za brak należytych zabezpieczeń w obszarze IT security. Brak adekwatnych zabezpieczeń był przyczyną wycieku danych osobowych na bardzo dużą skalę. Chodziło o nieco ponad 2 mln rekordów.

Spółka oczywiście odwołała się od niekorzystnej decyzji do Wojewódzkiego Sądu Administracyjnego. Jednak i w tym przypadku WSA uznał, że decyzja UODO pozostaje w mocy.

Kara dla SGGW – czyli coś dla IOD i nie tylko

Trzecia z decyzji, wydana względem SGGW jest zdecydowanie najmniej medialna. Kara jest relatywnie nieduża (50 tys. zł). Wyciek danych (ok. 100 tys. rekordów) też nie robi takiego wrażenia jak sprawa Morele.net. Dlaczego więc, w ogóle wspominam o tej decyzji UODO?

To pierwsza decyzja, w której UODO tak szczegółowo odniósł się do relacji IOD – Administrator Danych. Administrator Danych musi umożliwić IOD zapoznanie się z tym, co się aktualnie dzieje. IOD musi być wdrażany w bieżące i planowane procesy związane z ochroną danych osobowych.

Z własnego doświadczenia pamiętam sytuację sprzed kilku lat, kiedy jeszcze jako ABI, zostałem wdrożony w projekt budowy sklepu internetowego. Wszystko byłoby w jak najlepszym porządku, gdyby nie to, że o wszystkim dowiedziałem się… kiedy sklep już funkcjonował.

Takie sytuacje nie powinny mieć miejsca. Decyzja UODO tworzy przestrzeń dla Inspektorów Ochrony Danych i ułatwi skuteczną komunikację z Administratorem.

To także pierwsza decyzja, w której UODO zakwestionował sposób pełnienia funkcji IOD. Cenna wskazówka dla wszystkich IOD, mówiąca o tym, czego może oczekiwać od nich UODO.

Podsumowanie

Wskazane wyżej orzeczenia i decyzje niosą za sobą ważne konsekwencje praktyczne. Zamiast tradycyjnego podsumowania, tabela z wnioskami i działaniami, które warto podjąć w najbliższej przyszłości.

Decyzja/orzeczenie	Wniosek	Działanie
Aleksandrów Kujawski WSA utrzymuje karę 40 tys. zł w mocy	Umowy powierzenia są ważne, a obowiązek ich podpisania w pierwszej kolejności obciąża Administratora Danych.	Sprawdź rejestr umów powierzenia, zaktualizuj RCP. Jeśli brakuje Ci umów powierzenia – wyślij monit do Twoich kontrahentów. Powołaj się na decyzję UODO i orzeczenie WSA. W ostateczności, rozważ zakończenie współpracy w przypadku odmowy podpisania umowy powierzenia.
Morele.net WSA utrzymuje karę 2 830 410 zł w mocy	Ktoś musi jednoznacznie wziąć odpowiedzialność za obszar IT Security. Konieczne są audyty i ciągłe monitorowanie poziomu zabezpieczeń. Poziom zabezpieczeń powinien być stale podnoszony wraz z pojawianiem się nowych rozwiązań technologicznych.	Kto w Twojej organizacji odpowiada za obszar Security IT? Jeśli nie ma takiej osoby bądź osób, zadbaj o to, żeby je wyznaczyć. Ustal plan i procedury audytowania obszaru IT Security.

		Zarekomenduj zewnętrzny lub wewnętrzny audyt obszaru IT.
SGGW UODO nakłada karę w kwocie 50 tys. zł	IOD musi być wdrażany i zapoznawany z procesami ochrony danych osobowych. IOD powinien wypełniać swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania.	Jeśli jesteś IOD – masz prawo domagać się wdrażania Cię w procesy organizacji w której działasz. Jeśli czujesz, że nie zawsze jesteś informowany/a o ważnych procesach – ta decyzja na pewno ułatwi Ci życie. Pamiętaj też, że realizując swoje zadania, powinieneś stosować środki i metody dostosowane do specyfiki konkretnego Administratora Danych.
SGGW UODO nakłada karę w kwocie 50 tys. zł	IOD powinien zadbać o analizę ryzyka lub zaznaczyć Administratorowi Danych konieczność jej wykonania.	Zarekomenduj Administratorowi Danych wykonanie analiz ryzyka lub, w razie konieczności, samodzielnie rozpocznij działania w tym zakresie.
SGGW oraz Morele.net	Skala naruszenia ma znacznie. W przypadku SGGW, ok. 100 tys. rekordów. W przypadku Morele.net, ponad 2 mln rekordów.	Szczególnie dobrze zabezpiecz procesy prowadzone na dużą skalę. Zadbaj o analizę ryzyka, jeśli zajdzie taka konieczność, wykonaj DPIA. Pamiętaj też o zabezpieczeniach Security IT.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist

Źródła:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

- Decyzja Prezesa UODO z dnia 21 sierpnia 2020 r. ZSOŚS.421.25.2019
- Decyzja Prezesa UODO z dnia 10 września 2019 r. ZSPR.421.2.2019
- Decyzja Prezesa UODO z dnia 18 października 2019 r. ZSPU.421.3.2019
- Wyrok Wojewódzkiego Sądu Administracyjnego z 26 sierpnia 2020 r., sygn. akt II SA/Wa 2836/19 (Aleksandrów Kujawski)
- Wyrok Wojewódzkiego Sądu Administracyjnego z 3 września 2020 r., sygn. akt II Sa/WA 2559/19 (Morele.net)
- praktyczne doświadczenie budowania systemów ochrony danych osobowych od 2008 roku (jako ABI) i po 2018 roku (jako IOD)