Naruszenie ochrony danych osobowych byłego pracownika Rzecznika Finansowego

Wojewódzki Sąd Administracyjny podtrzymał decyzję Prezesa UODO, w której nałożono karę upomnienia na Rzecznika Finansowego za brak odpowiednich środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych.

Brak analizy ryzyka wiążącego się z korzystaniem przez pracowników z prywatnych komputerów podczas pracy zdalnej doprowadził do tego, że Rzecznik Finansowy nie wdrożył odpowiednich rozwiązań pozwalających należycie chronić przetwarzane dane, takich jak m.in. stosowne procedury i zabezpieczenia na wypadek kradzieży urządzenia. Taka sytuacja miała miejsce w przypadku komputera jednego z pracowników administratora, przez co doszło do naruszenia ochrony danych osobowych. Prezes UODO udzielił więc Rzecznikowi Finansowemu upomnienia, które wyrokiem z 5 października 2023 r. podtrzymał Wojewódzki Sąd Administracyjny w Warszawie.

Do naruszenia ochrony danych osobowych doszło w związku z kradzieżą prywatnego komputera byłego pracownika Rzecznika Finansowego. **W komputerze tym przechowywane były dane osobowe przetwarzane podczas pracy zdalnej świadczonej dla administratora danych. Fakt nieprzeprowadzenia przez administratora analizy ryzyka sprawił, że dane te nie zostały odpowiednio zabezpieczone. Ponadto administrator nie upewnił się, czy pracownik po zakończeniu świadczenia pracy skutecznie i trwale usunął dane z komputera. Brak odpowiednich zabezpieczeń technicznych i organizacyjnych doprowadził do nałożenia przez Prezesa UODO kary upomnienia na administratora.**

Skarżąc decyzję organu nadzorczego, Rzecznik Finansowy twierdził, iż skradziony komputer należał do byłego już pracownika, a Prezes UODO nie udowodnił, że na jego dysku twardym faktycznie znajdowały się dane osobowe. Skarżący podnosił też, że w postępowaniu administracyjnym nie ustalono, czy komputer był chroniony hasłem, a także wskazywał, że osoba świadcząca w przeszłości pracę dla Rzecznika Finansowego jest radcą prawnym, a więc odrębnym administratorem danych.
Żaden z powyższych argumentów nie został podzielony przez WSA w Warszawie. Wojewódzki Sąd Administracyjny nie miał wątpliwości, że administratorem danych w tym przypadku był Rzecznik Finansowy, a nie jego pracownik. Sąd rozstrzygając tę kwestię, przywołał definicję administratora zawartą w RODO, zgodnie z którą jest nim ten, kto decyduje o celach i sposobach przetwarzania danych osobowych. WSA podkreślił przy tym, że pracownik nie występuje jako odrębny podmiot prawa, a jego działania są działaniami pracodawcy, za które pracodawca ponosi odpowiedzialność. W ocenie Sądu nie zmienia tej sytuacji prawnej nawet działanie naruszające lub wykraczające poza zakres powierzonych pracownikowi zadań i obowiązków pracowniczych czy też status radcy prawnego byłego pracownika.
WSA w Warszawie zgodził się z Prezesem UODO, że administrator danych powinien przeprowadzić analizę ryzyka w związku z pracą zdalną pracowników i korzystaniem przez nich zarówno z prywatnych, jak i służbowych komputerów. Taka analiza wskazałaby na potrzebę zastosowania odpowiednich rozwiązań m.in. na wypadek kradzieży komputera, w którym są przetwarzane dane osobowe. Sąd uznał, że administrator uchybiając obowiązkom RODO w zakresie analizy ryzyka, jak i wdrożenia odpowiednich rozwiązań technicznych i organizacyjnych mających zapewniać bezpieczeństwo przetwarzanym danym, starał się przerzucić odpowiedzialność za to na pracownika. **Pomimo iż pracownik był zobowiązany do łączenia się przez VPN, korzystania z odpowiednich programów do szyfrowania plików oraz stosowania haseł do logowania znanych wyłącznie jemu i ich cyklicznej zmiany, to z umowy zawartej pomiędzy stronami nie wynika, by pracownik był zobowiązany do szyfrowania dysku twardego.**
Odpowiadając na zarzut skarżącego, że organ nadzorczy nie udowodnił w postępowaniu, iż komputer nie był odpowiednio chroniony, Sąd wskazał, iż ciężar dowodowy w tym przypadku spoczywa po stronie administratora i to on powinien być w stanie wykazać, że prywatny laptop pracownika został odpowiednio zabezpieczony przed potencjalnym nieuprawnionym dostępem do danych osobowych, które się na nim znajdowały.
W swoim orzeczeniu WSA zwrócił też uwagę, że administrator nie zweryfikował również, czy pracownik skutecznie usunął dane z komputera. Sąd uznał także, że gdyby przyjęte przez Rzecznika Finansowego rozwiązania były skuteczne, to fakt kradzieży komputera jego byłemu pracownikowi nie miałby żadnego wpływu na bezpieczeństwo procesu przetwarzania danych osobowych.

Zdaniem Sądu Prezes UODO prawidłowo zastosował upomnienie, biorąc pod uwagę działania podjęte przez administratora zaraz po naruszeniu ochrony danych osobowych.