Warszawa, dn. 30.01.2025 r.

Analiza ryzyka a kara finansowa dla ZHP

Instruktor ZHP zostawił w metrze plecak z laptopem należącym do Chorągwi Stołecznej ZHP. Prezes Urzędu Ochrony Danych Osobowych nałożył na Chorągiew karę w wysokości 24 555 zł za to, że nie zastosowała środków technicznych i organizacyjnych odpowiadających ryzyku dla danych przetwarzanych na przenośnych komputerach.

Od lat jestem związana ze Stowarzyszeniem ZHP, co sprawia, że jego działalność i misja są mi dobrze znane. W naszej organizacji non-profit stawiamy na elastyczność i otwartość, co oznacza, że wprowadzanie zasad, jak te, które często obowiązują w firmach prywatnych jest zwyczajnie niemożliwe. RODO jednak dotyczy i obowiązuje również w ZHP.

Zgubienie laptopa to zdarzenie niewątpliwie losowe. Nie ma w tym nic niezwykłego, ponieważ każdemu z nas może zdarzyć się taka historia. W takiej sytuacji jednak ważnych jest kilka innych aspektów. Istotne jest, aby administrator zastosował odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych oraz ochrony przed nieautoryzowanym dostępem. Odpowiednie działania w tym zakresie są kluczowe dla minimalizacji ryzyka i ochrony prywatności użytkowników. Temat ten pojawia się w dyskusjach bardzo często, jednak zazwyczaj jest bagatelizowany i nie traktowany z należytą uwagą. Pamiętajmy, że środki w celu zapewnienia bezpieczeństwa danych będą, a na pewno powinny być dobrane indywidulnie do organizacji. Czy w takiej organizacji jak ZHP jesteśmy / powinniśmy być w stanie przewidzieć powyższą sytuację?

Wróćmy do sedna sprawy, a więc do omawianego przypadku, w którym zaginął laptop.

Naruszenie ochrony danych, które skutkowało nałożeniem kary przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO), miało miejsce, gdy instruktor Związku Harcerstwa Polskiego (ZHP) pozostawił w metrze plecak z laptopem należącym do Chorągwi. Na komputerze znajdowały się dane osobowe (w tym dane wrażliwe) takie jak: nazwiska i imiona członków organizacji, dane rodziców, daty urodzenia, adresy zamieszkania, numery PESEL, adresy e-mail, numery dowodów osobistych, numery telefonów, informacje dotyczące zdrowia oraz inne dane, takie jak przynależność do stowarzyszenia czy przydziały służbowe. Te informacje są kluczowe dla funkcjonowania ZHP. Przede wszystkim, aby zostać członkiem organizacji, konieczne jest gromadzenie danych nie tylko dzieci, ale także ich rodziców, w celu uzyskania zgody na przynależność. Ponadto, ZHP angażuje się w różnorodne działania oraz projekty, co wiąże się z pozyskiwaniem danych osób trzecich, zarówno w kontekście dotacji, jak i organizacji letnich czy zimowych akcji harcerskich. W związku z tym, organizacja przetwarza znaczne ilości danych osobowych, co podkreśla znaczenie ich starannej ochrony.

W powyższym przypadku PUODO wskazał, że administrator musi nie tylko wdrożyć środki ochrony, ale także regularnie testować, mierzyć i oceniać ich skuteczność. **Analiza ryzyka jest niezwykle ważna dla każdego ADO - nie chodzi tu o konkretny przypadek zostawienia laptopa w metrze. Chodzi o to, w jaki sposób administrator dobrał zabezpieczenia do przetwarzania danych elektronicznych na laptopach.** Szczególnie istotne jest to, że urządzenia były transportowane i wykorzystywane w różnych lokalizacjach, co miało miejsce niejednokrotnie. Dotychczasowe środki ochrony uznano za niewystarczające. W przypadku laptopa zabezpieczeniem było jedynie hasło do systemu operacyjnego. Dysk laptopa nie był szyfrowany.

Sięgając bezpośrednio do przepisów RODO, należy przyjąć za punkt wyjścia art. 24: *„Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane”*. Przepis ten nie wskazuje wprost w jaki sposób zabezpieczyć laptopa, ale należy pamiętać, że szyfrowanie jako metoda zabezpieczenia danych zostało wskazane w art. 32 ust. 1 lit. a RODO. Szyfrowanie dysków w laptopach staje się coraz bardziej powszechne i jest prostsze niż kiedykolwiek. Wiele systemów operacyjnych oferuje wbudowane funkcje szyfrowania, które umożliwiają użytkownikom łatwe zabezpieczenie swoich dysków. Na przykład, w systemie Windows można skorzystać z BitLockera, natomiast użytkownicy macOS mają do dyspozycji FileVault. Alternatywnie, dostępny jest także darmowy program VeraCrypt, który umożliwia szyfrowanie dysków w różnych systemach operacyjnych.

Oprócz wdrożenia wymagań PUODO przez Chorągiew Stołeczną oraz ogólnie w organizacji ZHP, uważam, że niezwykle ważne jest kontynuowanie edukacji i podnoszenie świadomości wśród osób zajmujących się przetwarzaniem danych osobowych. Konieczne jest również dokładne przemyślenie, kto ma dostęp do tych danych w tak szerokim zakresie oraz dążenie do maksymalnego ograniczenia liczby takich osób.

Olga Skotnicka – ekspert ds. ochrony danych osobowych w iSecure Sp. z o.o.