

Kategoria: Aktualności

Opublikowano: środa, 19, kwiecień 2023 08:01

Joanna Gryboś-Chechelska

Odśłony: 899

Urząd Ochrony Danych Osobowych nałożył administracyjną karę pieniężną w wysokości ponad 33 tys. zł na administratora, który utracił poufność danych osobowych. Ponadto organ nadzorczy nakazał mu zaprzestać powierzania przetwarzania danych podmiotowi, z którym współpracował na podstawie umowy zawierającej braki. Jak wykazało postępowanie, zarówno administrator, jak i podmiot przetwarzający naruszyli przepisy RODO, bo nie wdrożyli odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych.

Do UODO wpłynęło zgłoszenie naruszenia ochrony danych osobowych, polegające na utracie poufności danych. Administrator w zgłoszeniu podał również dane podmiotu przetwarzającego zajmującego się kompleksową obsługą informatyczną. Niezależnie od powyższego, UODO pozyskał też informację z przekazów medialnych o naruszeniu ochrony danych osobowych, znajdujących się m.in. w polisach ubezpieczeniowych potwierdzających zawarcie z różnymi towarzystwami ubezpieczeniowymi umów ubezpieczenia w okresie od maja 2015 r. do listopada 2020 r., które były publicznie dostępne w zasobach informatycznych należących do administratora. Administrator potwierdził, że zgłoszenie naruszenia ochrony danych osobowych przekazane UODO dotyczy tego samego zdarzenia, które zostało opisane przez media.

Jak ustalono, do naruszenia doszło podczas wydzielenia wspólnego zasobu roboczego zawierającego repozytorium plików i udostępnienia go pracownikom w sieci lokalnej oraz zdalnie.

Obowiązki administratora – analiza ryzyka

Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo tym danym, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”), a administrator uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, powinien wdrożyć odpowiednie środki techniczne i organizacyjne. Co ważne, środki te są w razie potrzeby poddawane przeglądowi i uaktualniane. Wymienione obowiązki ciąży nie tylko na administratorach, ale też na podmiotach przetwarzających.

Środki techniczne i organizacyjne

Ustalenie odpowiednich środków technicznych i organizacyjnych jest procesem dwuetapowym. W pierwszej fazie należy określić poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych, a w drugiej należy ustalić, jakie środki techniczne i organizacyjne będą właściwe, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

W przedmiotowej sprawie należało zbadać, czy podmioty dokonały analizy ryzyka, a także czy na jej podstawie określiły oraz zastosowały środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa danych osobowych odpowiadający temu ryzyku. W ocenie UODO takiej ukierunkowanej analizy jednak nie przeprowadzono, poprzestając jedynie na ogólnych założeniach. Wyjaśnienia zarówno administratora, jak i podmiotu przetwarzającego wskazywały na to, że podmioty te stosują jedynie regulacje wewnętrzne administratora m.in. działają na podstawie Polityki ochrony danych osobowych. Brak przeprowadzonej analizy ryzyka poskutkował doбором nieadekwatnych środków.

Oprócz analizy ryzyka, wdrożenia środków organizacyjnych i technicznych, ważna jest ich

Kategoria: Aktualności

Opublikowano: środa, 19, kwiecień 2023 08:01

Joanna Gryboś-Chechelska

Odsłony: 899

weryfikacja

Równie ważne jak prawidłowy dobór środków technicznych i organizacyjnych, uwzględniający możliwe ryzyka, jest ich weryfikowanie i ustalenie, czy wprowadzane zmiany są prawidłowe. Takie działanie podmiotów zobowiązanych pozwoliłoby uniknąć naruszenia ochrony danych osobowych. Obowiązki podmiotów uczestniczących w procesie przetwarzania danych osobowych nie powinny – w ocenie organu nadzorczego – kończyć się na przeprowadzeniu analizy ryzyka i zastosowaniu odpowiednich środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzanych danych osobowych.

Brak takiej weryfikacji, wobec niewdrożenia odpowiednich środków technicznych i organizacyjnych skutkowało w tej sprawie wystąpieniem przedmiotowego naruszenia. Pewne działania weryfikacyjne zostały przeprowadzone dopiero po wystąpieniu naruszenia ochrony danych osobowych.

Podmiot przetwarzający powinien zapewnić gwarancje

Administrator korzystający z usług podmiotów przetwarzających powinien upewnić się, czy podmioty te zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

W tej sprawie weryfikacja kompetencji podmiotu przetwarzającego nie miała charakteru sformalizowanego, ponieważ polegała na przeprowadzeniu rozmowy, a świadczone przez podmiot usługi nie budziły zastrzeżeń administratora. Zdaniem UODO pozytywnie oceniana współpraca stanowić może jedynie punkt wyjścia przy dokonywaniu weryfikacji, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Samo podpisanie umowy powierzenia przetwarzania danych osobowych bez dokonania właściwej oceny podmiotu przetwarzającego nie może być uznane za realizację obowiązku przeprowadzenia postępowania weryfikującego podmiot przetwarzający. Wyznacznikiem dla takiej oceny nie może być jedynie wieloletnia współpraca i korzystanie z usług danego podmiotu przetwarzającego.

W niniejszej sprawie zmiany w systemie informatycznym nie zostały wprowadzone na podstawie określonych procedur, a prawidłowość ich przebiegu nie została zweryfikowana po ich dokonaniu. Ze względu na niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych, również na podmiot przetwarzający została nałożona administracyjna kara pieniężna. Administrator nie zweryfikował sposobu realizacji przez podmiot przetwarzający zmian w systemie informatycznym, w którym przetwarzane były dane osobowe. Zdaniem UODO takie działanie znacząco obniżyłoby ryzyko uzyskania dostępu przez osoby nieuprawnione do danych przetwarzanych w tym systemie, a tym samym zminimalizowałoby ryzyko naruszenia praw lub wolności osób fizycznych.

Źródło: ip