Bezpieczeństwo bez półśrodków

Skuteczne zarządzanie ochroną danych w firmie

W TYM WYDANIU:

LexDigital

lexdigital.pl

Jakub Pawłowski
Legal Counsel

Pseudonimizacja i anonimizacja

Precedensowa sprawa w TSUE

Przed Trybunałem Sprawiedliwości Unii Europejskiej (TSUE) zawisł bardzo interesujący spór dotyczący pojęcia pseudonimizacji i anonimizacji danych osobowych. Sprawa pod sygnaturą C-413/23, bo o niej mowa, oraz zaproponowane w opinii Rzecznika Generalnego rozstrzygnięcie mogą mieć istotny wpływ na status prawny danych przekazywanych pomiędzy podmiotami przetwarzającymi.

Stan faktyczny sprawy

Sprawa w dużym skrócie dotyczy przetwarzania danych osobowych akcjonariuszy i wierzycieli hiszpańskiego banku, który przeszedł proces restrukturyzacji i uporządkowanej likwidacji. W ramach tego procesu konieczne było oszacowanie, czy akcjonariusze i wierzyciele otrzymaliby lepsze traktowanie w przypadku standardowej procedury niewypłacalności. Do tego celu organ UE, a konkretnie Jednolita Rada ds. Restrukturyzacji i Uporządkowanej Likwidacji (SRB), przekazała dane osobowe firmie audytorskiej, która miała przeprowadzić odpowiednią wycenę.

Głównym punktem spornym jest to, czy SRB dopełniła obowiązku informacyjnego, wynikającego z rozporządzenia (UE) 2018/1725, względem tych akcjonariuszy i wierzycieli. **Europejski Inspektor Ochrony Danych (EIOD) argumentuje, że nawet jeśli dane zostały poddane pseudonimizacji, to nadal podlegają przepisom o ochronie danych osobowych.** W związku z tym SRB, wg EIOD, miała obowiązek powiadomić osoby, których dane dotyczyły, o przekazaniu ich danych firmie audytorskiej.

Stan faktyczny i problem, który musi rozstrzygnąć TSUE sprowadza się zatem do tego, czy dane, które są spseudonimizowane dla podmiotu A mogą stracić swój osobowy charakter po przekazaniu ich do podmiotu B. Innymi słowy, problem dotyczy tego, pod jakimi warunkami dane te będą uznawane za dane osobowe lub nieosobowe z perspektywy podmiotu B.

Przepisy podlegające interpretacji

Warto podkreślić, że sprawa nie jest rozpatrywana w kontekście RODO, lecz na kanwie *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. U. UE. L. z 2018 r. Nr 295, str. 39)*, czyli innymi słowy „RODO", tyle że dotyczącego organów publicznych UE.

Pomimo tego, że jest to odrębny od akt prawny jest on w swojej konstrukcji i treści wręcz bliźniaczy do RODO. Oczywiście są różnice, jednak kluczowe z perspektywy ochrony danych osobowych oraz przedmiotowej sprawy pojęcia i instytucje są tożsame.

Pseudonimizacja a anonimizacja

Zrozumienie kontekstu sprawy wymaga wyjaśnienia dwóch pojęć. Pierwszym z nich jest pseudonimizacja.

Pseudonimizacja

Zgodnie z definicją legalną, "pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Anonimizacja

Drugim pojęciem jest anonimizacja, która w przeciwieństwie do pseudonimizacji nie posiada definicji legalnej, jednak jest powszechnie rozumiana jako nieodwracalny proces przekształcania danych osobowych w taki sposób, aby uniemożliwić ich powiązanie z konkretną osobą fizyczną. Zasady ochrony danych nie powinny bowiem mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować.

O co spiera się EIOD i SRB?

Sama różnica pomiędzy pseudonimizacją i anonimizacją jest dosyć prosta do uchwycenia. **Pseudonimizacja jest bowiem procesem odwracalnym, a anonimizacja już nie.** Gdy pseudonimizujemy dane zawsze mamy przynajmniej dwa zbiory danych, które dzięki dodatkowym informacjom (np. indywidualnemu kodowi) możemy ze sobą powiązać.

Sęk tkwi natomiast w tym, że do tej pory dosyć zgodnie przyjmowano, że w przypadku pseudonimizacji te dwa rozdzielone zestawy informacji nadal są danymi osobowymi, niezależnie od tego gdzie i przez kogo lub w czyim imieniu są przetwarzane.

Ww. stanowisko konsekwentnie prezentuje w zawisłej przez TSUE sprawie EIOD, który uważa, że nawet dane, które zostały spseudonimizowane (czyli zmodyfikowane w taki sposób, aby trudniej było zidentyfikować konkretne osoby bez dodatkowych informacji), nadal podlegają przepisom o ochronie danych osobowych. EIOD podkreśla, że wymóg rzetelnego i przejrzystego przetwarzania danych ma kluczowe znaczenie, nawet w kontekście danych spseudonimizowanych.

Zgoła odmienne stanowisko zajmuje natomiast SRB, która uważa, że jeżeli najpierw doszło do pseudonimizacji danych i w stosunku do tak przetworzonych danych – co istotne przekazanych innemu podmiotowi – reidentyfikacja poszczególnych jest niemożliwa przez ten podmiot, to dane te nie powinny być automatycznie traktowane jako "dane osobowe" w sposób, który nakładałby na administratora pełny obowiązek informacyjny.

Stanowisko Rzecznika Generalnego

Sprawa staje się jeszcze bardziej ciekawa, gdy spojrzy się na opinię Rzecznika Generalnego w tej sprawie. Gwoli wyjaśnienia, w sprawach przed TSUE Rzecznik Generalny nie jest sędzią, lecz pełni funkcję opiniodawcy i merytorycznego sprawozdawcy. Praktyka pokazuje, że opinie Rzeczników Generalnych w większości przypadków są aprobowane przez składy orzekające i stanowią kanwę rozstrzygnięcia.

W komentowanej sprawie Rzecznik Generalny argumentuje, że dane spseudonimizowane, które są przekazywane stronom trzecim (w tym przypadku firmie audytorskiej), nie powinny być automatycznie uznawane za dane osobowe w rozumieniu przepisów, jeśli ryzyko ponownej identyfikacji osób jest "nieistniejące lub nieznaczne". Oznacza to, że jeśli odbiorca danych nie ma środków ani możliwości, aby powiązać spseudonimizowane dane z konkretnymi osobami, to dla tego odbiorcy dane te nie są danymi osobowymi w pełnym tego słowa znaczeniu, co ma wpływ na obowiązek informacyjny.

Rzecznik Generalny podkreślił w opinii, że kluczowe jest to, czy odbiorca spseudonimizowanych danych ma dostęp do dodatkowych informacji, które umożliwiłyby mu ponowną identyfikację osób. Jeśli takiego dostępu nie ma, to dla odbiorcy dane te nie są danymi osobowymi, a tym samym obowiązek informacyjny spoczywający na administratorze może być w tym zakresie ograniczony lub nieistniejący.

Stanowisko Rzecznika stoi zatem w kontrze do poglądów prezentowanych przez EIOD, popieranego dodatkowo przez Europejską Radę Ochrony Danych.

edpb
European Data Protection Board

Jakie będzie rozstrzygnięcie tej sprawy oczywiście na ten moment nie wiadomo, jednak jeżeli TSUE przyjmie stanowisko Rzecznika Generalnego za swoje, to będzie to swoista rewolucja w ochronie danych osobowych, która może przyczynić się do usprawnienia wielu procesów biznesowych opartych o wymianę danych. Potwierdzenie, że spseudonimizowane dane, które zostaną przekazane stronom trzecim nie mającym możliwości reidentyfikacji, nie powinny być automatycznie uznawane za dane osobowe może mieć kluczowe znaczenie chociażby dla trenowania algorytmów i rozwoju AI oraz procesów wymiany informacji pomiędzy przedsiębiorcami.

Dariusz Janiak
Information Security & Data Protection Expert

Bezpieczeństwo bez półśrodków

Jak skutecznie wdrożyć SZBI?

Niektóre organizacje utrzymują komórki bezpieczeństwa informacji, inne posiadają pewne elementy służące ochronie danych osobowych, ale bardzo często brakuje w tych działaniach kompleksowego, przemyślanego systemu. Podczas audytów zerowych w różnych firmach zauważamy, że pomimo wytwarzania znacznych ilości dokumentów regulujących kwestie bezpieczeństwa informacji organizacja nie działa w sposób uporządkowany i systemowy.

Po co mi SZBI?

Po co wdrażać System Zarządzania Bezpieczeństwem Informacji (SZBI)? Pobudek może być wiele i każda prawdopodobnie będzie uzasadniona.

Taka decyzja może wynikać ze świadomości zagrożeń, zwłaszcza cyberataków.

Ważnym argumentem może być zapewnienie zgodności z regulacjami jak RODO, DORA, NIS 2 czy aktualizowaną ustawą o KSC.

Powodem wdrożenia SZBI mogą być także korzyści wizerunkowe – certyfikat ISO 27001, określający wymagania SZBI to uznana, międzynarodowa gwarancja dbałości o bezpieczeństwo pożądana często przez klientów i kontrahentów.

Niezależnie od powodu, jeśli podejmiemy decyzję, że wdrażamy System Zarządzania Bezpieczeństwem Informacji, to zróbmy to dobrze, ograniczając do minimum półśrodki.

Zagrożenia ewoluują, coraz bardziej do głosu dochodzą te związane z wykorzystywaniem sztucznej inteligencji, w tym:

Zaawansowane ataki phishingowe naśladujące styl komunikacji ofiary

Automatyzacja ataków ransomware, które w bardzo szybki sposób mogą zidentyfikować podatności potencjalnych celów

Algorytmy omijania zabezpieczeń

Deepfake

Działając w takim otoczeniu Twoja firma jest narażona na na negatywne skutki oddziaływania

wskazanych zagrożeń. Ich konsekwencje mogą być bardzo poważne: od bolesnych strat wizerunkowych i konieczności wypłaty odszkodowań do dotkliwych kar administracyjnych.

Jak skutecznie wdrożyć SZBI?

Jaki zatem powinien być system, który ochroni organizację przed dotkliwymi konsekwencjami zagrożeń dla bezpieczeństwa informacji? Odpowiedź wydaje się być prosta: musi być to system, który jest wdrożony skutecznie oparty na odpowiedniej strukturze i kompetencjach, takich jak:

- zarządzanie zagrożeniami,
- interpretowanie wyników oceny ryzyka
- monitorowanie podatności w systemach teleinformatycznych i budowanie na ich podstawie algorytmów postępowania.

Dla skutecznego wdrożenia SZBI kluczowe jest zwłaszcza zaangażowanie kierownictwa. Bez tego organizacja nie będzie czuła, że kwestie bezpieczeństwa rzeczywiście są ważne.

System daje korzyści

W LexDigital regularnie wspieramy firmy we wdrażaniu Systemów Zarządzania Bezpieczeństwem Informacji m.in. w oparciu o wymagania Normy ISO 27001. Okazuje się, że dobrze funkcjonujący system poza poprawą bezpieczeństwa informacji wpływa także pozytywnie na skuteczność realizowanych procesów w organizacji.

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI