Warszawa, 20.02.2025 r.

Wysoka kara dla firmy gromadzącej dane z platformy LinkedIn czyli KASPR ukarany za nielegalne gromadzenie danych – 240 000 euro grzywny

Wstęp

Nie dalej jak pół roku temu w artykule pt. „Tworzenie baz danych na podstawie profilów osób na portalach branżowych typu LinkedIn w kontekście przetwarzania danych osobowych i zgodności z RODO" przedstawiłem praktyczny poradnik w jaki sposób gromadzić dane z wykorzystaniem baz danych dostępnych m .in. na portalach branżowych typu LinkedIn. W treści publikacji zwróciłem uwagę na problem Scraping'u danych tj. praktyki polegającej na automatycznym zbieraniu danych z profili użytkowników za pomocą narzędzi, systemów IT, czyli technicznie bardzo skutecznych narzędzi, ale często spotykających się z problemami natury prawnej tak w zakresie naruszania warunków użytkowania (regulaminów) portali branżowych jak i przepisów dotyczące ochrony danych.
Nie długo trzeba było czekać, aby sprawą niewłaściwego scraping'u zajął się jeden z organów nadzoru. Tym razem padło na francuski organ nadzorczy ds. ochrony danych osobowych, czyli CNIL (Commission Nationale de l'Informatique et des Libertés), który nałożył karę finansową na firmę KASPR.
W telegraficznym skrócie – ww. firma oferowała rozszerzenie do przeglądarki Chrome, umożliwiające pozyskiwanie danych kontaktowych użytkowników LinkedIn. CNIL stwierdził liczne naruszenia RODO, w tym przetwarzanie danych bez podstawy prawnej, co skutkowało grzywną w wysokości 240 000 euro.
Sprawa KASPR jest jednym z największych ostrzeżeń dla firm zajmujących się przetwarzaniem danych osobowych bez zgody użytkowników. CNIL podkreślił, że nielegalne pozyskiwanie i przechowywanie danych stanowi poważne naruszenie, mogące prowadzić do wysokich kar finansowych oraz utraty reputacji. W dobie rosnącej świadomości dotyczącej ochrony prywatności użytkowników takie działania są coraz częściej wykrywane i sankcjonowane.

Jak działał KASPR?

KASPR dostarczał użytkownikom płatne narzędzie do pozyskiwania danych kontaktowych osób odwiedzanych na LinkedIn. W wyniku tej działalności firma zgromadziła bazę zawierającą około 160 milionów kontaktów. Dane te były wykorzystywane do celów sprzedażowych, rekrutacyjnych i weryfikacji tożsamości.
CNIL ustalił, że KASPR zbierał informacje nie tylko z profili publicznych, ale również tych, których użytkownicy świadomie ograniczyli widoczność dla kontaktów pierwszego i drugiego stopnia. Organ uznał, że takie działanie było bezprawne i naruszało prywatność użytkowników LinkedIn.

Model biznesowy KASPR

Głównym celem działania KASPR było umożliwienie przedsiębiorcom i rekruterom łatwego dostępu do informacji kontaktowych „profesjonalistów" na LinkedIn. Narzędzie pozwalało klientom na przeszukiwanie bazy danych i uzyskiwanie numerów telefonów oraz adresów e-mail osób, które niekoniecznie chciały udostępniać te informacje publicznie.
Jednym z kluczowych problemów było to, że KASPR agregował dane z wielu źródeł, w tym z serwisów typu Whois, GitHub, często łącząc je w sposób sprzeczny z wolą użytkowników. Wiele osób nie miało świadomości, że ich dane zostały zgromadzone i są udostępniane osobom trzecim.

Działalność firmy wywołała falę skarg użytkowników, którzy byli kontaktowani przez nieznane im podmioty, wykorzystujące ich dane do celów komercyjnych. Wielu z nich poczuło się oszukanych i wykorzystanych bez ich wiedzy, w konsekwencji czego zgłosiło sprawę do CNIL, co doprowadziło do wszczęcia postępowania i nałożenia kary.

Naruszenia RODO

Podczas dochodzenia CNIL zidentyfikował szereg naruszeń przepisów o ochronie danych osobowych:

1. **Brak podstawy prawnej do przetwarzania danych (art. 6 RODO)** – KASPR przetwarzał dane użytkowników LinkedIn, w szczególności również tych którzy ograniczyli ich widoczność. CNIL uznał, że naruszało to ich uzasadnione oczekiwania dotyczące prywatności.
2. **Nieproporcjonalnie długi okres przechowywania danych (art. 5 ust. 1 lit. e RODO)** – Firma przechowywała dane przez 5 lat od każdej aktualizacji profilu użytkownika, co prowadziło do nadmiernie długiego przetwarzania danych.
3. **Brak przejrzystości w informowaniu użytkowników (art. 12 i 14 RODO)** – Firma przez cztery lata działania nie informowała osób, których dane gromadziła. Gdy zaczęła to robić w 2022 roku, używała wyłącznie języka angielskiego, co utrudniało odbiorcom zrozumienie komunikatu.
4. **Nieprawidłowe realizowanie prawa dostępu do danych (art. 15 RODO)** – Osoby, które chciały dowiedzieć się, skąd pochodzą ich dane, otrzymywały ogólnikowe odpowiedzi. KASPR nie wskazywał dokładnych źródeł pozyskania informacji.
5. **Nieprzestrzeganie prawa użytkowników do sprzeciwu wobec przetwarzania danych** – Użytkownicy, których dane zostały zgromadzone, nie mieli skutecznej możliwości ich usunięcia ani sprzeciwu wobec przetwarzania.

Jak widać, w przypadku KASPR wykorzystanie technik scrapingu bez wiedzy i zgody użytkowników, a także brak jasnych zasad retencji danych, doprowadziły do licznych naruszeń prawa, co znalazło odzwierciedlenie w decyzji CNIL.

Konsekwencje dla KASPR

CNIL nałożyła na KASPR grzywnę w wysokości 240 000 euro oraz zobowiązała firmę do:

- zaprzestania zbierania danych użytkowników, którzy ograniczyli ich widoczność,
- usunięcia już zgromadzonych danych lub poinformowania użytkowników o możliwości sprzeciwu wobec przetwarzania,
- zaprzestania automatycznego odnawiania okresu przechowywania danych,
- dostarczania użytkownikom informacji o przetwarzaniu ich danych w języku, który rozumieją,
- podawania szczegółowych informacji na temat źródeł pozyskania danych.

Firma otrzymała termin do 18 czerwca 2025 roku na dostosowanie się do przepisów, w przeciwnym razie grożą jej dalsze kary finansowe.

Czego możemy się nauczyć z tej sprawy?

Przypadek KASPR stanowi ostrzeżenie dla wszystkich firm zajmujących się przetwarzaniem danych osobowych oraz korzystających z zewnętrznych baz danych. Kluczowe wnioski płynące z tej sprawy to:

- **Respektowanie ustawień prywatności użytkowników** – Jeśli użytkownik ogranicza widoczność swoich danych, firmy muszą respektować ten wybór.
- **Transparentność w komunikacji** – Informacje o przetwarzaniu danych muszą być jasne, łatwo dostępne i podane w zrozumiałym języku.

- **Zachowanie proporcjonalności** – Dane nie mogą być przechowywane w nieskończoność; ich retencja musi być zgodna z pierwotnym celem przetwarzania.
- **Prawidłowa realizacja prawa dostępu** – Osoby, których dane są przetwarzane, mają prawo wiedzieć, skąd one pochodzą i kto je gromadzi.
- **Przestrzeganie zasad etyki biznesowej** – Firmy korzystające z danych osobowych powinny działać zgodnie z najwyższymi standardami etycznymi, aby unikać naruszeń praw konsumentów.

Jak wskazano w artykule dotyczącym przetwarzania danych z LinkedIn, firmy podczas wdrażania polityk i procedur zgodne z zasadami "privacy by design" i "privacy by default", aby uniknąć podobnych problemów prawnych powinny podejmować poniższe działania:

- Korzystanie z oficjalnych narzędzi rekrutacyjnych platform takich jak LinkedIn,
- Upewnienie się, że podmioty z bazy są informowane o sposobach i celach przetwarzania ich danych,
- Regularne przeprowadzanie audytów zgodności z RODO, w tym obejmujących podmioty zewnętrzne dostarczające bazy danych,
- Stosowanie wyłącznie legalnych źródeł danych i weryfikacja dostawców informacji (ankiety zgodności z ODO).

Podsumowanie

Sprawa KASPR pokazuje, że europejskie organy nadzorujące ochronę danych coraz surowiej egzekwują przepisy RODO. Firmy korzystające z publicznych danych muszą postępować zgodnie z przepisami, aby uniknąć poważnych konsekwencji prawnych i finansowych. Działalność niezgodna z regulacjami RODO może skutkować wysokimi karami i utratą zaufania klientów.

Ponadto sprawa ta podkreśla rosnącą świadomość użytkowników w zakresie ochrony prywatności. Coraz więcej osób zwraca uwagę na sposób, w jaki ich dane są gromadzone i wykorzystywane, co wymusza na firmach większą przejrzystość i odpowiedzialność.

Paweł Wojciechowski – adwokat, specjalista ds. ochrony danych osobowych iSecure Sp. z o.o.

Źródło:

- *https://www.cnil.fr/en/data-scraping-kaspr-fined-eu240000*
- *https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000050791828*