Podział obowiązków i odpowiedzialności między administratorem a procesorem w kontekście naruszenia ochrony danych osobowych

dr Gabriela Bar

https://www.linkedin.com/in/gabrielabar/

Studium przypadku i kilka spostrzeżeń na tle decyzji Prezesa UODO w sprawie Fortum

Zgodnie z **decyzją Prezesa UODO ze stycznia 2022 r.:**

- Fortum jako administrator nie zaimplementowała odpowiednich środków technicznych i organizacyjnych gwarantujących bezpieczeństwo przetwarzanych danych osobowych, co doprowadziło do naruszenia ich poufności oraz nie przeprowadziła należytej weryfikacji procesora danych, aby upewnić się, że ten zapewnia wystarczające gwarancje ochrony danych zgodnie z wymogami rodo.
- W rezultacie Spółka została ukarana karą administracyjną w wysokości **4 911 732 złotych** za naruszenie artykułów 5 ust. 1 lit. f, 24 ust. 1, 25 ust. 1, 28 ust. 1 oraz 32 ust. 1 i 2 rodo.

Studium przypadku i kilka spostrzeżeń na tle decyzji Prezesa UODO w sprawie Fortum

- Procesor Pika Sp. z o.o., również została ukarana za niezaimplementowanie odpowiednich środków technicznych i organizacyjnych, które zapewniałyby bezpieczeństwo danych osobowych, w tym ich poufność. Za to naruszenie, na firmę nałożona została kara w wysokości **250 135 złotych**, związana z naruszeniem artykułu 32 ust. 1 i 2 rodo, w kontekście artykułu 28 ust. 3 lit. c i f.

Naruszenie przepisów postępowania i nieustalenie stanu faktycznego

- Incydent będący przedmiotem postępowania związany był z faktem wprowadzenia **niewielkiej zmiany** w środowisku informatycznym dla usługi archiwum cyfrowego prowadzonego dla Fortum przez podmiot przetwarzający.
- **Fortum nie zlecała żadnych działań związanych z przetwarzaniem danych**, a jedynie potrzebę przyspieszenia działania serwerów. Operacja taka nie miała związku z danymi, a jedynie – z wydajnością sprzętu i oprogramowania bazy danych.
- Procesor obowiązującej między Stronami procedury nie dochował, nie skonsultował z Fortum rozwiązania, które ostatecznie zastosował, a nawet **nie poinformował, że przystępuje do jego realizacji**.

Naruszenie przepisów postępowania i nieustalenie stanu faktycznego

- Do incydentu doszło w wyniku tzw. **błędu ludzkiego** odpowiednio wykwalifikowanego pracownika podmiotu przetwarzającego. Nie był to zatem błąd systemowy, wynikający z niewłaściwej organizacji współpracy, braku procedur lub technicznych zabezpieczeń, ale sytuacja jednostkowa polegająca na braku uruchomienia firewalla.
- Prezes UODO nie ustalił, na czym dokładnie polegało naruszenie danych osobowych, w tym tego, czy jakiekolwiek dane osobowe „wyciekły” z bazy danych, której naruszenie dotyczyło ani jakie to były rzeczywiście dane.

Naruszenie przepisów postępowania i nieustalenie stanu faktycznego

WSA w Warszawie stwierdził w **wyroku z 10 października 2022 r.**, że:

- **Prezes UODO nie ustalił stanu faktycznego sprawy oraz oparł się jedynie na oświadczeniach stron złożonych w trakcie postepowania administracyjnego, bez dokonania ich weryfikacji**.
- Podstawowym obowiązkiem Prezesa UODO było ustalenie, czy Fortum prowadziło nadzór nad zmianami w systemie informatycznym elektronicznego archiwum oraz czy w sprawie doszło do wycieku danych, czy też jedynie krótkotrwałej możliwości uzyskania dostępu do danych osobowych przez osobę nieuprawnioną – **brak bowiem własnych ustaleń Prezesa UODO co do skutków naruszeń**.

Zapewnienie bezpieczeństwa danych przez administratora

- Zapewnienie odpowiedniego bezpieczeństwa wymaga podjęcia stosownych (proporcjonalnych) środków zabezpieczenia danych.
- **Nie muszą to być środki najlepsze z możliwych** (najdroższe, najbardziej zaawansowane technologicznie), powinny one być odpowiednie do zagrożeń i pozwalać na zapewnienie skutecznej ochrony.
- Wykazanie spełnienia wymogów z art. 28 ust. 1 wymagać może wymiany stosownych dokumentów np. polityk prywatności, warunków świadczenia usług, procedur zarządzania danymi, polityk bezpieczeństwa informacji, raportów z zewnętrznych audytów, uzyskanych certyfikatów (EROD w Wytycznych 07/2020).

Wybór odpowiedniego procesora

- Z przepisów rodo, w tym zwłaszcza z art. 28 ust. 1 rodo nie wynika konieczność przeprowadzenia jakiegoś **zorganizowanego postępowania weryfikacyjnego procesora**, z którego to należy sporządzić konkretny dokument.
- Praktyka do takiej sformalizowanej weryfikacji często zmierza w ślad za żądaniami Prezesa UODO, ale biorąc pod uwagę treść art. 28 ust. 1 rodo, w przepisie tym chodzi nie tyle o udokumentowane przeprowadzenia działań weryfikacyjnych, co o stwierdzenie przez administratora, że **procesor spełnia wymogi** wynikające z rodo.

Wybór odpowiedniego procesora

- Wystarczające gwarancje, o których mowa w art. 28 ust. 1 rodo i przeświadczenie o ich istnieniu mogą wynikać z **wieloletniej harmonijnej współpracy, która nie była naznaczona jakimikolwiek incydentami bezpieczeństwa**. Wbrew twierdzeniom Organu, fakt ten powinien być decydujący dla oceny, że podmiot przetwarzający spełnia wymogi z art. 28 ust. 1 rodo.

Wybór odpowiedniego procesora

- EROD w Wytycznych 07/2020 wprost wskazała, że ocena przez administratora, czy gwarancje są wystarczające, jest **formą oceny ryzyka**, która w dużej mierze będzie zależeć od rodzaju przetwarzania powierzonego podmiotowi przetwarzającemu i musi być dokonywana indywidualnie dla każdego przypadku, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz zagrożenia dla praw i wolności osób fizycznych.
- W konsekwencji EROD nie przedstawia **wyczerpującego wykazu** dokumentów lub działań, które podmiot przetwarzający musi pokazać lub wykazać w danym scenariuszu, ponieważ w dużej mierze zależy to od konkretnych okoliczności przetwarzania.

Wybór odpowiedniego procesora

- Zdaniem EROD, aby ocenić, czy gwarancje są wystarczające, administrator powinien wziąć pod uwagę następujące elementy: **wiedza ekspercka przetwarzającego** (np. wiedza techniczna w zakresie środków bezpieczeństwa i naruszeń danych); niezawodność procesora; zasoby procesora. **Reputacja podmiotu przetwarzającego na rynku może być również istotnym czynnikiem do rozważenia przez administratorów**.

Specjalistyczne kompetencje procesora i ich brak u administratora

- Charakter świadczonej przez procesora usługi może **nie dawać technicznych możliwości** sprawdzenia zastosowanych rozwiązań technicznych i wykonywanych prac programistycznych, gdyż korzystanie z tych usług odbywa się w modelu SaaS.
- Model SaaS przerzuca obowiązki instalacji, zarządzania, aktualizacji, pomocy technicznej z klienta na **dostawcę usługi**. W efekcie to dostawca ma kontrolę nad oprogramowaniem i obowiązek zapewnienia ciągłości jego działania.

Specjalistyczne kompetencje procesora i ich brak u administratora

- Administrator danych **nie ma więc co do zasady technicznej możliwości weryfikacji** całej listy kontrolnej czynności jakie musi wykonać administrator systemu czy programista, aby sprawdzić czy wprowadzone zmiany były przeprowadzone poprawnie od strony sieciowej (internet) lub programistycznej konfiguracji środowiska aplikacyjnego.
- **Są to podstawowe obowiązki dostawcy usług, jakich wymaga się od podmiotu działającego w profesjonalnym obrocie**.

Specjalistyczne kompetencje procesora i ich brak u administratora

- Czy można oczekiwać od Fortum jako przedsiębiorstwa sprzedającego paliwo gazowe i energię, aby w zakresie, w jakim nie posiada stosownych kompetencji, decydowała o zastosowanych środkach bezpieczeństwa i nadzorowała **drobiazgowo** podmiot przetwarzający?
- Nawet testowanie działania oprogramowania przez użytkownika jakim jest Fortum, nie gwarantuje i nie gwarantowała wykrycia błędu programisty jakim było **pozostawienie niezabezpieczonego portu komunikacyjnego (brak firewall)**, przez który mógł nastąpić nieuprawniony dostęp.
- Czy cykliczne audyty i inspekcje u procesora mogły takiemu błędowi zapobiec (pracownik procesora zadziałał wbrew politykom i instrukcjom procesora)?

Odpowiedzialność administratora czy procesora

- **Żaden przepis nie wyłącza stosowania art. 429 kc w odniesieniu do odpowiedzialności z tytułu powierzenia przetwarzania danych osobowych**.
- Przepisy o ochronie danych osobowych wyraźnie stanowią, że podmiot przetwarzający dane na zlecenie odpowiada za naruszenie obowiązków związanych z zabezpieczeniem danych tak jak administrator danych. Zaakceptowanie stanowiska prezentowanego przez SN mogłoby w praktyce oznaczać podważenie zasadności zawierania umów powierzenia przetwarzania danych, gdyż w każdym przypadku administrator danych ponosiłby pełną odpowiedzialność za naruszenia, których dopuścił się podmiot przetwarzający na jego zlecenie, **nawet w sytuacji, gdyby administrator dołożył szczególnej staranności przy wyborze podmiotu przetwarzającego oraz wyraźnie określił zakres i cel przetwarzania w umowie powierzenia**. Taki kierunek nie sposób uznać za słuszny nie tylko na gruncie Kodeksu cywilnego, ale również w świetle przepisów o ochronie danych osobowych (P. Fajgielski, Glosa do wyroku SN z dnia 1 czerwca 2017 r., I CSK 597/16, OSP 2018, nr 10, s. 98).

Odpowiedzialność administratora czy procesora

- Czy jeśli administrator podjął wszelkie niezbędne i możliwe w danym stanie faktycznym działania wymagane od niego na podstawie art. 24 ust. 1 i art. 32 ust. 1 i 2 rodo, to **za naruszenie samodzielnie odpowiadać powinien podmiot przetwarzający?**

Dziękuję za uwagę

dr Gabriela Bar

https://www.linkedin.com/in/gabrielabar/