Warszawa, 27.02.2025 r.

# Raportować incydenty – czyli łatwo powiedzieć a coraz trudniej zapanować - analiza projektu ustawy o systemach sztucznej inteligencji i nowego podejścia PUODO

Projekt ustawy o systemach sztucznej inteligencji zakłada wprowadzenie kompleksowych regulacji dotyczących bezpieczeństwa AI. Jednym z kluczowych elementów ma być nowy system zgłaszania poważnych incydentów. Ze względu na przewidziane wysokie kary za naruszenia, warto już teraz przeanalizować proponowane wymogi i rozpocząć przygotowania do ich wdrożenia.

## Ograniczony zakres podmiotowy

Projektowane przepisy nie obejmą wszystkich podmiotów wykorzystujących AI.
Zgodnie z art. 2 ust. 1 ustawy, który odwołuje się do art. 2 ust. 1 rozporządzenia 2024/1689, obowiązek raportowania dotyczy przede wszystkim dostawców systemów AI stosowanych w krytycznych obszarach. Należą do nich systemy wykorzystywane m.in. do:

- Oceny ryzyka i podejmowania decyzji wpływających na prawa jednostek - na przykład systemy oceniające zdolność kredytową, systemy rekrutacyjne czy rozwiązania wpływające na dostęp do świadczeń publicznych.
- Zarządzania infrastrukturą krytyczną - w tym systemy sterowania ruchem, zarządzania sieciami energetycznymi czy kontroli procesów przemysłowych mogących wpływać na bezpieczeństwo.
- Świadczenia usług medycznych - obejmuje to systemy diagnostyczne, systemy wspomagania decyzji klinicznych czy rozwiązania do analizy badań obrazowych.
- Edukacji i oceny kompetencji - w szczególności systemy służące do oceny uczniów i studentów lub decydujące o dostępie do edukacji.
- Identyfikacji biometrycznej - zwłaszcza systemy działające w czasie rzeczywistym w przestrzeni publicznej.

Co istotne, ustawa wprowadza wyłączenia z tego obowiązku. Zgodnie z art. 2 ust. 1 pkt 1, nie obejmie on osób fizycznych wykorzystujących systemy AI wyłącznie do celów osobistych, niezwiązanych z działalnością gospodarczą czy zawodową.
Dodatkowo art. 4 wyłącza spod regulacji systemy AI używane w obszarze obronności narodowej oraz przez służby specjalne. Nie podlegają jej również systemy wykorzystywane wyłącznie do celów badawczych i rozwojowych, o ile nie są testowane w warunkach rzeczywistych.
Warto zaznaczyć, że klasyfikacja systemu jako "wysokiego ryzyka" będzie wymagała szczegółowej analizy jego zastosowania i potencjalnego wpływu na prawa podstawowe, zdrowie i bezpieczeństwo osób. Sam fakt wykorzystania AI nie jest wystarczający - kluczowe znaczenie ma kontekst i skala potencjalnego oddziaływania systemu.

## Proponowana procedura zgłaszania incydentów

Projekt ustawy przewiduje bardzo krótki, 24-godzinny termin na zgłoszenie poważnego incydentu do Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (dalej: Komisja AI). To znacznie mniej niż przy naruszeniach ochrony danych osobowych regulowanych przez RODO. Zgłoszenie będzie musiało zawierać szczegółowe informacje o podmiocie, dokładny opis incydentu wraz z jego skalą i skutkami oraz podjęte działania zaradcze. Projektodawca wymaga też bieżącego aktualizowania tych informacji w miarę rozwoju sytuacji.

**Współpraca z PUODO**

Szczególnie interesującym aspektem projektu jest sytuacja, gdy incydent w systemie AI dotyczy również danych osobowych. Powstanie wtedy obowiązek podwójnego raportowania - do Komisji ds. AI oraz do PUODO, przy czym terminy i wymagany zakres informacji będą różne. To pokazuje, jak złożone może być zarządzanie incydentami w praktyce.

Kluczowe elementy współpracy między Organami wg projektu ustawy obejmują:

- Przepis art. 5 ust. 3 pkt 3 - Komisja współpracuje z Prezesem UODO w zakresie spraw dotyczących ochrony danych osobowych, w szczególności w sprawach, o których mowa w art. 57 ust. 10 oraz art. 74 ust. 8 rozporządzenia 2024/1689.
- Art. 80 ust. 1 pkt 4 - Przewodniczący Komisji może przekazywać Prezesowi UODO informacje o zgłoszonych poważnych incydentach związanych z wykorzystaniem systemów sztucznej inteligencji.
- Art. 113 - do ustawy o ochronie danych osobowych dodaje się art. 59a stanowiący: "Prezes Urzędu współpracuje z Komisją Bezpieczeństwa i Rozwoju Sztucznej Inteligencji".

PUODO zatem oprócz zgłoszeń od Administratorów, może zacząć otrzymywać zgłoszenia o naruszeniach dotyczących systemów AI wysokiego ryzyka również od Komisji AI.

**Czy PUODO ma zasoby, żeby obsłużyć je wszystkie?**

W tym kontekście warto zwrócić uwagę na zmieniające się podejście Prezesa Urzędu Ochrony Danych Osobowych (PUODO) do kwestii zgłaszania naruszeń. Jak wynika z najnowszych rekomendacji, PUODO zaleca, aby administratorzy zgłaszali również naruszenia **niskiego ryzyka w ciągu standardowych 72 godzin** od ich wykrycia.

Jest to istotna zmiana w stosunku do dotychczasowej interpretacji art. 33 RODO, który wymaga zgłaszania naruszeń jedynie wtedy, gdy mogą one skutkować ryzykiem naruszenia praw lub wolności osób fizycznych. Prezes UODO stoi na stanowisku, że administratorzy często nieprawidłowo oceniają poziom ryzyka, co prowadzi do niezgłaszania incydentów, które faktycznie powinny zostać zgłoszone. W praktyce oznacza to, że administratorzy powinni zgłaszać praktycznie wszystkie stwierdzone naruszenia ochrony danych osobowych, chyba że są w stanie jednoznacznie wykazać brak jakiegokolwiek ryzyka (co w praktyce jest rzadkością). Takie podejście znacząco zwiększa obciążenie administratorów, którzy muszą być przygotowani na znacznie częstsze raportowanie incydentów.

**Rekomendowane działania przygotowawcze**

Mimo że mamy do czynienia z projektem ustawy, który może jeszcze ulec zmianom, warto już rozpocząć przygotowania. Organizacje powinny przeanalizować, które z wykorzystywanych systemów AI mogą podlegać regulacji i rozpocząć prace nad procedurami wykrywania i zgłaszania incydentów. Szczególną uwagę należy zwrócić na koordynację działań w przypadku naruszeń dotyczących również danych osobowych oraz włączenie w definicje incydentów tych – związanych z systemami sztucznej inteligencji.

W praktyce wdrożenie projektowanych wymogów będzie wymagało istotnych zmian organizacyjnych i dokumentacyjnych. Odpowiednie przygotowanie pozwoli nie tylko uniknąć potencjalnych kar, ale przede wszystkim realnych zagrożeń związanych z niewłaściwym funkcjonowaniem systemów AI.

Czy to nie za dużo? Gdzie szukać pomocy?

**Audyt systemów AI według ISO 42001**

Organizacje, które dostarczają lub wykorzystują systemy AI, szczególnie te potencjalnie klasyfikowane jako wysokiego ryzyka, powinny rozważyć przeprowadzenie audytu wewnętrznego

zgodnie z normą ISO 42001. Taki audyt pozwoli nie tylko przygotować się do nowych wymogów ustawowych, ale także zbudować kompleksowy system zarządzania AI.
Audyt według ISO 42001 obejmuje szereg kluczowych obszarów. Audytorzy zbadają, czy organizacja:

- prawidłowo zidentyfikowała wszystkie wykorzystywane systemy AI i ich zastosowania
- przeprowadziła rzetelną ocenę ryzyka uwzględniającą aspekty techniczne, prawne i etyczne
- wdrożyła odpowiednie mechanizmy monitorowania i kontroli
- posiada skuteczne procedury wykrywania i reagowania na incydenty
- zapewnia właściwe zarządzanie danymi wykorzystywanymi przez systemy AI
- odpowiednio dokumentuje procesy i decyzje związane z AI

Szczególnie istotnym elementem audytu jest weryfikacja gotowości organizacji do spełnienia wymogów raportowania incydentów. Audytorzy sprawdzą nie tylko same procedury, ale także praktyczne aspekty ich realizacji - od systemów monitoringu po kompetencje personelu.

**Podsumowanie**
Projektowana ustawa o systemach sztucznej inteligencji wprowadza istotne obowiązki w zakresie zgłaszania incydentów. Choć dotyczy głównie systemów wysokiego ryzyka, wszystkie organizacje wykorzystujące AI powinny śledzić proces legislacyjny i odpowiednio się przygotować.
Wdrożenie normy ISO 42001 może znacząco ułatwić to zadanie, zapewniając sprawdzone ramy dla systemu zarządzania AI. Z ciekawostek – jedyny model językowy, który pokusił się o zgodność z normą to **Claude od firmy Anthropic. I to z jego wsparciem powstał dzisiejszy artykuł** 😊
Regularne audyty według tej normy pomogą nie tylko w spełnieniu wymogów prawnych, ale przede wszystkim w budowaniu bezpiecznych i odpowiedzialnych zastosowań sztucznej inteligencji. Co przy okazji zwiększy bezpieczeństwo przetwarzanych danych osobowych w tych systemach.

**Magdalena Jacolik** – specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.

Komentowane źródła:

- Ustawa o systemach sztucznej inteligencji – projekt z dnia 05.02.2025r
- Obowiązki administratorów związane ze zgłaszaniem naruszeń ochrony danych osobowych – Poradnik na gruncie RODO, luty 2025