Warszawa, 14.05.2025 r.

Reagowanie na incydenty bezpieczeństwa powstałe w systemach administrowanych na poziomie grupy kapitałowej – podejście zgodne z RODO

Wstęp

W dzisiejszym świecie cyfrowym, gdzie firmy działają w ramach międzynarodowych grup kapitałowych, zarządzanie bezpieczeństwem danych osobowych staje się coraz bardziej złożone. Publikacja ma na celu przybliżenie tematu reagowania na incydenty bezpieczeństwa danych osobowych w sytuacji, gdy systemy IT są administrowane centralnie przez spółkę główną (najczęściej z zagranicy), a użytkownikami oraz Administratorami danych są spółki zależne (córki) lub oddziały lokalne.

Kontekst prawny – podstawy z RODO

Zgodnie z ogólnym rozporządzeniem o ochronie danych osobowych (RODO), każda organizacja przetwarzająca dane osobowe musi zapewnić ich bezpieczeństwo. Artykuł 32 RODO nakłada obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa odpowiadającego ryzyku.

Ponadto, zgodnie z artykułem 33 RODO, w przypadku naruszenia ochrony danych osobowych, Administrator danych ma obowiązek zgłoszenia incydentu do organu nadzorczego w ciągu 72 godzin od momentu stwierdzenia naruszenia, a w niektórych przypadkach – poinformowania osób, których dane dotyczą.

Zgodnie z RODO (art. 32 i 33), to Administrator danych – czyli zazwyczaj spółka lokalna – odpowiada za zapewnienie bezpieczeństwa danych osobowych oraz za zgłoszenie naruszenia do organu nadzorczego w ciągu 72 godzin od jego wykrycia. Problem pojawia się jednak wtedy, gdy systemy są zarządzane centralnie przez spółkę główną, a lokalna jednostka **nie ma dostępu do logów, nie widzi incydentów na czas ani nie może samodzielnie wprowadzać zabezpieczeń**. Oznacza to, że choć formalna odpowiedzialność spoczywa na lokalnym Administratorze, to w praktyce **nie ma on narzędzi, by wywiązać się z obowiązków wynikających z RODO**.

Taka sytuacja może prowadzić do realnych naruszeń przepisów, np.:

- **Zbyt późnego zgłoszenia incydentu**, bo centrala nie przekazała informacji na czas – co łamie 72-godzinny termin z art. 33 RODO.
- **Niewdrożenia odpowiednich zabezpieczeń**, bo lokalna spółka nie ma wpływu na konfigurację systemu, mimo że powinna je zapewnić zgodnie z art. 32.
- **Braku przejrzystości wobec osób, których dane dotyczą**, jeśli lokalny Administrator nie zna skali naruszenia i nie może rzetelnie poinformować poszkodowanych.
- **Braku ważnej umowy powierzenia przetwarzania**, gdy relacja z centralą nie została formalnie uregulowana – co oznacza, że dane są przetwarzane bez podstawy prawnej.

W efekcie lokalna spółka, choć podporządkowana decyzjom centrali, **może zostać pociągnięta do odpowiedzialności** za naruszenie przepisów, na które de facto nie miała wpływu.

Kto jest kim w strukturze grupy kapitałowej?

W praktyce bardzo często mamy do czynienia z następującym układem sił w ramach grup kapitałowych i wykorzystywanych systemów IT:

- Spółka córka / oddział lokalny – pełni rolę Administratora danych osobowych, ponieważ to ona decyduje o celach i środkach przetwarzania danych;
- Spółka główna (zagraniczna) – dostarcza i zarządza systemami IT dla całej grupy. W tym przypadku, co do zasady, pełni rolę Podmiotu przetwarzającego (Procesora), ponieważ przetwarza dane na zlecenie spółek zależnych.

Zgodnie z definicją RODO, to Administrator decyduje o celach i sposobach przetwarzania danych. Jednak w praktyce, w grupach kapitałowych, rola ta jest często ograniczona. Spółka główna – jako dostawca systemów – narzuca konkretne rozwiązania technologiczne, które są już na stałe zintegrowane z modelem biznesowym całej grupy. Tym samym lokalne spółki nie mają realnej możliwości wyboru alternatywnego sposobu przetwarzania danych, ponieważ ich działalność jest uzależniona od korzystania z określonych systemów IT.

W efekcie, zadanie Administratora sprowadza się często do zaakceptowania gotowych celów i sposobów przetwarzania, które są de facto już określone przez funkcjonalności narzucone przez centralę. Dobrym przykładem tego zjawiska są korporacyjne systemy HR, ERP czy CRM, których struktura, przepływy danych, integracje i mechanizmy bezpieczeństwa są projektowane i wdrażane na poziomie spółki głównej – bez możliwości ich zmiany przez spółki córki.

Przykład 1: lokalna spółka korzysta z systemu HR wdrożonego przez centralę, który automatycznie zbiera dane biometryczne pracowników przy wejściu do biura. Choć lokalne przepisy wymagają zgody na takie przetwarzanie, spółka nie ma możliwości technicznego wyłączenia tej funkcji bez decyzji centrali.

Przykład 2: centrala narzuca wykorzystanie chmurowej platformy CRM, której polityka retencji danych nie uwzględnia lokalnych przepisów o archiwizacji danych osobowych. Administrator lokalny nie ma wpływu na konfigurację platformy, mimo że odpowiada za zgodność z prawem lokalnym.

Największe wyzwania i problemy

A. Opóźniona komunikacja

W przypadku incydentu bezpieczeństwa (np. wyciek danych, dostęp nieuprawnionych osób, awaria systemu), spółka córka – jako Administrator – często dowiaduje się o tym z opóźnieniem. Dlaczego? Ponieważ:

- To spółka główna ma dostęp do logów systemowych;
- To ona analizuje ruch sieciowy i incydenty;
- Brakuje jasnych i szybkich kanałów raportowania do spółek lokalnych;

Przykład: W systemie kadrowym centralnie zarządzanym przez spółkę główną dochodzi do nieuprawnionego dostępu do profili pracowników z poziomu konta administratora technicznego. Spółka lokalna dowiaduje się o naruszeniu dopiero po tygodniu, gdy jeden z pracowników zauważa podejrzaną aktywność.

B. Ograniczona decyzyjność Administratora

Administrator danych powinien mieć kontrolę nad sposobem przetwarzania danych. Tymczasem:

- Nie ma pełnej wiedzy o konfiguracji systemów.
- Nie może samodzielnie zareagować (np. zablokować konta, zmienić ustawień).
- Musi czekać na reakcję Procesora.

Przykład: W systemie sprzedażowym występuje luka umożliwiająca podgląd danych klientów przez osoby nieuprawnione. Spółka lokalna nie może samodzielnie zastosować łaty bezpieczeństwa – musi zgłosić to do centrali i czekać kilka dni na wdrożenie poprawki.

C. Brak umowy powierzenia danych (lub jej niekompletność)

Zdarza się, że w grupie kapitałowej nie ma formalnej umowy powierzenia przetwarzania danych (DPA – Data Processing Agreement), albo jest ona zbyt ogólna. Skutki?

- Brak wytycznych co do zgłaszania incydentów.
- Brak kar za opóźnienia w reakcji.
- Trudności w egzekwowaniu obowiązków.

Przykład: W jednej ze spółek ujawnione zostają dane klientów w związku z błędem w integracji systemów CRM. Nie wiadomo, kto odpowiada za zgłoszenie incydentu – spółka lokalna nie ma dostępu do pełnych danych logowania, a centrala nie traktuje sytuacji jako naruszenia, co prowadzi do zaniechania zgłoszenia do organu nadzorczego.

D. Różnice kulturowe i językowe

Współpraca między spółką główną a lokalnymi oddziałami bywa utrudniona z powodu różnic językowych, braku znajomości lokalnego prawa i zwyczajów biznesowych.

Przykład: Spółka główna z Azji wysyła powiadomienia o incydencie technicznym w formacie i języku niezrozumiałym dla oddziałów europejskich, co skutkuje brakiem reakcji lokalnych Administratorów przez kilkanaście godzin.

E. Brak spójności w ocenie incydentów i ograniczony dostęp do informacji

Częstym problemem w grupach kapitałowych jest fakt, że spółki zależne otrzymują wyłącznie ograniczone informacje o incydentach, często w formie oficjalnych stanowisk przygotowanych przez centralę. Powoduje to:

- Utrudnienia w dokonaniu samodzielnej oceny ryzyka.
- Brak dostępu do dokumentacji technicznej i logów.
- Konieczność dostosowania treści zgłoszenia do PUODO do wersji uzgodnionej przez centralę.

Przykład: Dochodzi do ataku ransomware na wspólny system HR. Spółka główna po 48 godzinach przekazuje okrojoną notatkę, w której nie stwierdzono utraty danych. Lokalny Administrator nie otrzymuje szczegółowych danych technicznych i nie jest w stanie samodzielnie ocenić konieczności zgłoszenia incydentu do PUODO, mimo że przetwarzane były dane jego pracowników.

Dobre praktyki – co można zrobić?

A. Jasny podział ról i odpowiedzialności

W dokumentach takich jak umowa powierzenia przetwarzania, polityka bezpieczeństwa i procedury reagowania należy jasno określić:

- Kto odpowiada za monitoring systemów i wykrywanie incydentów.
- Kto i w jakim terminie przekazuje informacje o incydencie do lokalnych Administratorów.
- Kto odpowiada za kontakt z organem nadzorczym i kiedy inicjowane są zgłoszenia.

B. Automatyzacja raportowania i alertów

Systemy IT powinny umożliwiać automatyczne wykrywanie anomalii (np. nietypowe logowania, szyfrowanie danych, wzorce malware) i generowanie powiadomień kierowanych jednocześnie do centrali i lokalnych Administratorów. Alerty powinny być opatrzone technicznymi szczegółami niezbędnymi do oceny skali naruszenia.

C. Szkolenia i ćwiczenia scenariuszowe

Spółki w grupie powinny cyklicznie:

- Organizować wspólne szkolenia z zakresu reagowania na incydenty oraz współpracy między centralą a jednostkami lokalnymi.
- Ćwiczyć wybrane scenariusze (np. symulacja wycieku danych z systemu HR), w tym również weryfikować kanały komunikacji i czas reakcji.

D. Lokalne punkty kontaktowe ds. incydentów

W każdej spółce zależnej warto wyznaczyć osobę (np. lokalnego DPO lub Security Officer), która będzie:

- Odpowiedzialna za bieżącą analizę informacji o incydentach.
- Pełnić rolę łącznika z centralą.
- Koordynować lokalne działania w przypadku naruszeń.

E. Transparentność i niezależność oceny ryzyka

Administratorzy danych w jednostkach lokalnych powinni mieć dostęp do pełnych danych technicznych oraz możliwość niezależnego dokonania oceny ryzyka – nawet jeśli centrala uzna, że incydent nie wymaga zgłoszenia. Każdy z nich odpowiada bowiem za dane, które przetwarza jako Administrator, i musi działać w zgodzie z lokalnym prawem.

F. Wspólny zestaw narzędzi i ujednolicone procedury

- Udostępnienie wspólnego repozytorium (np. w intranecie), gdzie znajdują się aktualne procedury, checklisty i kontakty.
- Stworzenie centralnej procedury raportowania incydentów, która uwzględnia możliwość zgłoszeń równoległych przez różne spółki.

G. Umożliwienie dostępu do danych audytowych i logów

Systemy centralne powinny być projektowane w sposób zapewniający lokalnym Administratorom dostęp do dzienników systemowych, historii działań oraz logów dotyczących przetwarzania danych w ich obszarze odpowiedzialności. Dzięki temu możliwa jest szybka analiza i reakcja na incydenty.

H. Włączenie lokalnych jednostek w testy bezpieczeństwa

Testy bezpieczeństwa, takie jak testy penetracyjne czy oceny ryzyka, powinny uwzględniać lokalne warunki. Lokalne zespoły (np. DPO, IT) powinny być aktywnie zaangażowane w planowanie i realizację testów, aby lepiej odzwierciedlić rzeczywiste zagrożenia i sposoby reagowania.

I. Dostępność dokumentacji w lokalnych językach

Procedury reagowania na incydenty, checklisty oraz instrukcje powinny być dostępne w językach lokalnych. Ułatwia to szybkie działanie i minimalizuje ryzyko błędów wynikających z nieporozumień językowych.

J. Koordynacja zgłoszeń do PUODO

Dla zapewnienia zgodności i transparentności, warto opracować procedurę koordynacji zgłoszeń do PUODO. Procedura ta powinna:

- Umożliwiać każdej spółce samodzielne dokonanie zgłoszenia, jeśli zachodzi taka potrzeba.
- Przewidywać dołączanie stanowiska centrali do zgłoszenia, jako element wspierający, nie ograniczający decyzyjności lokalnego Administratora.

Podsumowanie – jak uniknąć "bycia na łasce Procesora"?

W grupie kapitałowej bardzo często to spółka główna rozdaje karty – dostarcza narzędzia, zarządza infrastrukturą, kontroluje dane. Jak widać na podstawie powyżej przyjętego scenariusza, jednak z perspektywy RODO, to lokalna spółka, jako Administrator danych, ponosi pełną odpowiedzialność prawną za bezpieczeństwo przetwarzania danych osobowych.

Aby uniknąć sytuacji, w której lokalna jednostka staje się bezradnym wykonawcą decyzji centrali, należy przyjąć aktywną postawę i zbudować fundamenty rzeczywistego wpływu na bezpieczeństwo danych. W szczególności warto:

- **Zidentyfikować kluczowe luki w obecnym modelu zarządzania bezpieczeństwem** – np. brak umowy powierzenia, niepełna wiedza o systemach, utrudniony dostęp do logów czy brak wpływu na reakcję w razie incydentu. Audyt takich obszarów powinien być punktem wyjścia.
- **Zawalczyć o zapisanie w dokumentacji formalnych ścieżek eskalacji i zgłaszania incydentów, które będą funkcjonować niezależnie od decyzji centrali** – nawet wbrew niej, jeśli interes osób, których dane dotyczą, tego wymaga.
- **Ustalić minimalny zakres niezależności technicznej i organizacyjnej,** np. poprzez:
    - dostęp lokalnych Administratorów do systemów monitorujących,
    - możliwość tymczasowego zablokowania konta użytkownika,
    - samodzielne zgłoszenie naruszenia do organu nadzorczego, bez konieczności zatwierdzenia przez centralę.
- **Zbudować sieć lokalnych DPO (Inspektorów Ochrony Danych), którzy będą współpracować, ale nie działać w zależności od jednej,** nadrzędnej jednostki. Ich zadaniem powinno być wspieranie, doradzanie, ale i egzekwowanie przestrzegania lokalnego prawa, nawet jeśli oznacza to wejście w spór z centrą.
- **Upowszechniać świadomość prawną i techniczną wśród kadry zarządzającej** – szczególnie w kontekście realnej odpowiedzialności karnej, finansowej i reputacyjnej, jaka ciąży na spółce lokalnej. W razie incydentu to ona występuje przed organem nadzorczym, a nie centrala.
- **Oceniać systemy IT nie tylko pod kątem funkcjonalnym, ale też zgodności z lokalnym prawem ochrony danych**, nawet jeśli są one narzucane z góry. W razie potrzeby, należy zgłaszać zastrzeżenia na piśmie, aby udokumentować brak zgody na ryzykowne rozwiązania – co może stanowić ważny dowód w przypadku postępowania kontrolnego.

Wreszcie – **lokalna spółka nie powinna bać się zadawania trudnych pytań swojej centrali**. Czy mamy plan reagowania na incydenty? Czy mamy kopie zapasowe? Czy wiemy, kto i kiedy podejmuje decyzje o zgłoszeniu incydentu? Czy znamy ścieżkę komunikacji w razie kryzysu?

RODO nie zabrania centralizacji systemów IT – ale nakłada obowiązek, aby każdy Administrator danych faktycznie mógł realizować swoje obowiązki.

Dlatego:

budujmy mosty – ale z barierkami ochronnymi,

delegujmy kompetencje – ale nie odpowiedzialność,

współpracujmy – ale nie kosztem prawa.

Tylko wtedy można mówić o rzeczywistej zgodności z RODO, a nie o jej symulacji.

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