Warszawa, 21.05.2024 r.

Hic sunc dracones – o czym powinien pamiętać deweloper w kontekście RODO?

„HC SVNT DRACONES" (łac. *hic sunt dracones* – „tu są smoki") to termin, który czasem można było znaleźć na średniowiecznej czy renesansowej mapie – naniesiony w miejscu, o którym autor mapy nic nie wiedział. Ten brak wiedzy oczywiście skutkowało założeniem, że są tam wszelkiej materii potwory

morskie, smoki niczym ten na globusie z 1508 roku, czy ludzie z jedną nogą i wielką stopą kryjący się w cieniu tej stopy pod palącym Słońcem. Można go czytać jako symbol strachu przed nieznanym.
Po 6 latach stosowania RODO takich niezbadanych krain ze smokami zostało niewiele. Na przypadającą w sobotę 25 maja rocznicę obowiązywania rozporządzenia 2016/679 napiszemy o tym, na co przedsiębiorcy z branży deweloperskiej powinni szczególnie uważać w 2024 roku. Są to:

- brak lub nieaktualna analiza ryzyka,
- niewłaściwy nadzór nad procesorami,
- współpraca w ramach grupy kapitałowej.

Analiza ryzyka

Z licznych audytów w zakresie ochrony danych osobowych, które przeprowadził autor tego artykułu wynika niestety, że analizy ryzyka pozostają wysoce problematycznym obszarem dla wielu przedsiębiorstw. Przez „wysoce problematyczny" rozumiem, że wiele firm albo nie ma ich wcale, albo zrobiło ją raz przy wdrożeniu RODO (najpowiewniej w 2018 roku) i nigdy nie aktualizowało.
Dlaczego analiza ryzyka jest ważna? Praktyka orzecznicza Prezesa UODO (jak również publikacje na jego stronie internetowej i nasze doświadczenia w reprezentacji Klientów w razie incydentu) pokazują, że jest to jeden z pierwszych obszarów, które są analizowane w razie kontroli. Informując o niedawnej decyzji o nałożeniu kary na Politechnikę Warszawską UODO wskazał, iż „*zastosowanie środków technicznych bez dokonania uprzedniej analizy ryzyka dla procesu przetwarzania danych osobowych nie może dawać gwarancji, że zastosowane środki będą skuteczne i adekwatne*". Podobne stanowisko znalazło się w decyzji o nałożeniu kary na P. Sp. z o.o.

Problematyczne jest również posiadanie nieaktualnej analizy ryzyka – może ona dawać złudne poczucie bezpieczeństwa. Złudne, bo z upływem czasu zmieniają się nie tylko zagrożenia (w 2018 roku dopiero nieśmiało pojawiała się powszechna dziś metodyka „Big Game Hunting" w stosowaniu ransomware), ale również i organizacja, która ową analizę przeprowadziła.

Błędem jest też traktować analizę ryzyka wyłącznie jako papierek, którzy trzeba „odbębnić" czy „odhaczyć" dla zapewnienia zgodności z przepisami. Dobrze przeprowadzona, jest niezwykle cennym narzędziem dla uniknięcia incydentu o bardzo poważnych (finansowo, wizerunkowo i operacyjnie) konsekwencjach. Analiza ryzyka udziela też odpowiedzi na pytanie które obszary bezpieczeństwa wymagają wzmocnienia w pierwszej kolejności. Takie oparte na danych podejście do alokacji zasobów pozwala odpowiednio priorytetyzować inwestycje w bezpieczeństwo.

Nadzór nad procesorami

We współczesnych realiach gospodarczych trudno znaleźć firmę, która nie korzysta z żadnych usług dostarczanych przez podmioty zewnętrzne. Obsługa księgowo - kadrowa, IT, archiwizacja dokumentów, headhunting, marketing internetowy to tylko niektóre procesy, które często zlecane są w ramach outsourcingu. I wszystkie te działania wymagają zawarcia umowy powierzenia przetwarzania danych osobowych. Po 6 latach stosowania RODO świadomość prawna w tym zakresie zdecydowanie zmierza we właściwym kierunku i coraz rzadziej trafiamy na tego typu współprace realizowane bez zawarcia obowiązkowej umowy powierzenia przetwarzania danych osobowych. Ale z perspektywy wymogów ochrony danych osobowych, taka umowa to dopiero drugi krok w relacji administratora z procesorem. Zgodnie z art. 28 ust. 3 lit. h RODO, administrator danych ma prawo kontrolować przestrzeganie przepisów prawa przez procesora. Prawo to powiązane jest z

obowiązkiem realnego sprawowania tego nadzoru, a Prezes UODO wielokrotnie dał do zrozumienia, że poważnie traktuje zaniechania w tym obszarze.

Nie można mieć w świetle powyższego wątpliwości, że jakiś nadzór nad procesorem musi być. Pytanie zatem brzmi: jaki?

Jedną z największych zalet (ale chyba i jednocześnie wad) RODO jest to, że wymogi tam zawarte są skalowalne. Oznacza to, że inny nadzór powinien być sprawowany nad zewnętrznym headhunterem (który sporadycznie przetwarza tylko podstawowe dane zawarte w dokumentach CV) a inny nad firmą, która dostarcza nam wsparcie IT (a więc ma codzienny, pełny dostęp do absolutnie wszystkich danych, jakie przetwarza nasza firma). Inaczej kontrolujemy zewnętrzną firmę księgową, a inaczej – spółkę matkę, która w ramach grupy kapitałowej prowadzi obsługę księgową spółek celowych założonych do realizacji poszczególnych inwestycji. W dobraniu zakresu i sposobu kontroli pomoże nam dobrze zrobiona analiza ryzyka. A w praktyce, o ile z bieżącej współpracy nie dostajemy niepokojących sygnałów o procesorze, w większości przypadków powinna wystarczyć kontrola procesora polegająca na cyklicznym rozsyłaniu ankiet do samooceny. Takie działania nie wiążą się ze znacznym wysiłkiem organizacyjnym i kosztami, a pozwalają trzymać rękę na pulsie i podejmować działania prewencyjne (a nie reakcyjne).

Współpraca w ramach grupy kapitałowej

Coraz popularniejszym modelem działania w branży deweloperskiej jest tworzenie dla realizacji poszczególnych inwestycji tzw. spółek celowych. Zmniejsza to ryzyko biznesowe dla dewelopera – w przypadku nieoczekiwanego niepowodzenia inwestycji, koszty pozostaną w wydzielonej spółce, która „ochroni" spółkę matkę. Takie działanie pozwala też na uproszczenie i przyspieszenie podejmowania decyzji operacyjnych.

Zdarza się jednak, że twórcy takiej korporacyjnej struktury zupełnie zapominają o przepisach o ochronie danych osobowych. Oczywistym jest, że spółki w obrębie jednej grupy kapitałowej mają prawo wymieniać się danymi osobowymi na zasadzie swojego uzasadnionego interesu (art. 6 ust. 1 lit. f RODO). Ale takich transferów nie można opierać wyłącznie na tej „oczywistości". Muszą za nią iść odpowiednie procedury, analizy prawnie uzasadnionego interesu, stosowne umowy oraz klarowna informacja dla osób, których dane dotyczą. O wadze tej ostatniej przekonał się operator popularnego komunikatora WhatsApp (Meta Platfroms Inc.), na który właśnie za brak przejrzystości w przekazywaniu danych osobowych na podstawie uzasadnionego interesu nałożono karę w wysokości 225 mln Euro.

Korzystanie ze spółek celowych ma jednak zasadniczą wadę z perspektywy przepisów RODO. Jak szerzej napisała o tym niedawno na naszym blogu Olga Skotnicka, kary za naruszenie RODO w wysokości do 2-4% całkowitego rocznego obrotu firmy z poprzedniego roku liczone są dla obrotu całej grupy kapitałowej, a nie tylko dla danej spółki – córki.

Podsumowując

Po 6 latach obowiązywania RODO białych plam na mapach tego jak te przepisy stosować zostaje coraz mniej. Ten zmniejszający się stan niepewności nie oznacza jednak, że można spocząć na przysłowiowych laurach i zapomnieć o obowiązku ochrony danych osobowych. Zaniechania na tym odcinku nie tylko łączą się z ryzykiem nałożenia kar administracyjnych, ale przede wszystkim – wobec

rosnącej świadomości tych przepisów w społeczeństwie – mogą skutkować bardzo trudnymi do naprawienia stratami wizerunkowymi.

Daniel Taberski - radca prawny, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.

*[Grafika wygenerowana przez AI Canva Magic Studio™].