Warszawa, 11.07.2023 r.

Badanie Due Diligence spółki pod kątem ODO – dobre praktyki

Dlaczego warto zwrócić uwagę na kwestie ochrony danych osobowych przy badaniu Due Diligence?

Obecnie na rynku powszechną praktyką stało się włączanie obszaru ochrony danych osobowych do badania Due Diligence spółek (dalej „DD"). Przedmiotem badania jest, co do zasady, weryfikacja systemu ochrony danych osobowych spółki tj. ustalenie czy oraz w jaki sposób spółka wdrożyła obowiązujące regulacje z zakresu ochrony danych osobowych.

Prawidłowe wdrożenie RODO[1], bo do tego w uproszczeniu sprowadza się organizacja systemu ochrony danych osobowych w spółce, może mieć istotne znaczenie dla celów badania DD, obejmujących:

i. identyfikację nieprawidłowości związanych z działalnością badanej spółki;
ii. prawidłowe oszacowanie rzeczywistej wartości badanej spółki;

Przede wszystkim należy pamiętać, że nieprawidłowości w organizacji systemu ochrony danych osobowych wiążą się z ryzykiem naruszenia obowiązujących przepisów ochrony danych osobowych. Naruszenia mogą z kolei prowadzić m in. do konieczności zapłaty odszkodowań za poniesione szkody przez podmioty danych lub do nałożenia administracyjnych kar pieniężnych, w wysokości do 20 mln EUR albo 4 % całkowitego rocznego obrotu przedsiębiorstwa. Przykładem może być decyzja brytyjskiego organu nadzoru ICO ws. Marriot International Inc.[2] obrazująca ryzyko związane z nabyciem spółki bez przeprowadzenia dokładnego badania DD w zakresie bezpieczeństwa danych osobowych, wskutek której brytyjski organ nadzorczy nałożył karę w wysokości 18,4 miliona funtów na Marriott International Inc.

Z drugiej strony, niewdrożenie w organizacji systemu ochrony danych osobowych albo przeprowadzenie procesu wdrożenia w sposób błędny może wymagać poniesienia znacznych nakładów zarówno finansowych jak i czasowych dla naprawy takiego stanu rzeczy. Koszty związane z wdrożeniem RODO w organizacji zależą m. in. od jej wielkości, przedmiotu działalności oraz stopnia skomplikowania poszczególnych procesów obejmujących przetwarzanie danych osobowych i mogą wynosić nawet setki tysięcy złotych. Konieczność poniesienia przez potencjalnego nabywcę spółki dodatkowych kosztów w celu wdrożenia środków naprawczych, wpływa na szacowaną wartość badanej spółki, a w praktyce obniża jej wartość.

Ustalenia w powyższych względach mogą stanowić punkt wyjścia np.: do negocjacji warunków sprzedaży spółki. Zidentyfikowanie nieprawidłowości na tak wczesnym etapie

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

[2] https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf

jakim jest badanie DD może zasadniczo wpłynąć na opłacalność ewentualnej przyszłej transakcji.

Gdzie zacząć badanie DD?

Po pierwsze, od analizy udostępnionej dotychczas przez badaną spółkę dokumentacji – najczęściej w formie virtual data room („VDR") które pozwalają na udostępnianie dokumentów podmiotom przeprowadzającym badanie. Analizy przesłanych dokumentów nie należy ograniczać wyłącznie do tzw. „dokumentacji ODO", składającej się w szczególności z polityk, procedur, wytycznych, ale również zwrócić uwagę na pozostałe obszary badania DD. Podkreślenia wymaga, że system ochrony danych osobowych rozciąga się na całość działalności spółki, obejmując zarówno procesy wewnętrzne jak i zewnętrzne. Istotne informacje z perspektywy prawidłowego wdrożenia systemu ochrony danych osobowych w spółce mogą stanowić część dokumentacji m. in.:

i. w obszarze HR np.: w związku z przechowywaniem CV, stosowaniem monitoringu pracowniczego, upoważnieniami do przetwarzania danych;
ii. dotyczącej relacji korporacyjnych np.: sposobów i warunków przekazywania danych osobowych w grupie kapitałowej, w szczególności transgranicznego przetwarzania danych osobowych;
iii. w zakresie zobowiązań, w tym umowy z kontrahentami, dostawcami np.: przy korzystaniu z zewnętrznych rozwiązań IT (outsourcing);

Po drugie, komunikacja z członkami zespołu odpowiedzialnymi za badanie pozostałych obszarów. Warto zwrócić uwagę pozostałych zespołów, osób odpowiedzialnych za badanie poszczególnych obszarów działalności spółki na kwestie związane z ochroną danych osobowych. W ten sposób, możliwe jest szybsze zidentyfikowanie wszystkich istotnych kwestii z perspektywy ochrony danych osobowych składających się na system ochrony danych w badanej spółce.

Po trzecie, internet to dobre źródło wiedzy na początkowym etapie badania DD. Internet jest naturalnym polem dla interakcji badanej spółki z podmiotami danych, co może dostarczyć wielu istotnych informacji o działalności spółki na zewnątrz organizacji. Analiza publikowanych przez badaną spółkę informacji dotyczących ochrony danych osobowych, w szczególności sposób, forma ich publikowania oraz komunikacja z podmiotami danych składa się na ogólny obraz świadomości organizacyjnej spółki i stosowanie systemu ochrony danych osobowych. Dobrym źródłem informacji są publikowane polityki prywatności i ich analiza w kontekście funkcjonalności serwisu, klauzule informacyjne lub treści zgód marketingowych. Ponadto, na te elementy należy zwrócić szczególną uwagę, ponieważ są publiczne i łatwo dostępne, co oznacza, że potencjalnie nieograniczone grono odbiorców może zidentyfikować nieprawidłowości, naruszenia w ochronie danych osobowych a następnie dokonać zgłoszenia do organu nadzoru (PUODO). W wyniku zgłoszenia, organ nadzorczy może wszcząć postępowanie kontrolne względem spółki. W zależności od powagi zidentyfikowanych naruszeń w toku postępowania, organ może nałożyć administracyjne kary pieniężne, o których mowa w pierwszym podrozdziale, powyżej.

Jak przeprowadzić badanie DD oraz na co zwrócić uwagę?

Punkt wyjścia dla badania systemu ochrony danych osobowych w spółce stanowią, co do zasady, regulacje RODO. RODO zawiera szereg wymogów jakie musi spełniać spółka w ramach przetwarzania danych osobowych. Wymogi te związane są, w szczególności, z:

i. przestrzeganiem zasad przetwarzania danych osobowych;
ii. określeniem podstaw przetwarzania danych osobowych;
iii. realizacją praw podmiotów danych;
iv. bezpieczeństwem danych osobowych;
v. prowadzeniem dokumentacji ochrony danych osobowych w niezbędnym zakresie;
vi. przekazywaniem danych osobowych pomiędzy podmiotami (powierzenie przetwarzania, udostępnienie, współadministrowanie danymi);
vii. obowiązkami w zakresie transferów danych osobowych;

Warto zwrócić uwagę na praktyczne opracowania europejskich oraz krajowych organów w zakresie realizacji wymogów RODO, w szczególności Europejskiej Rady Ochrony Danych oraz Prezesa Urzędu Ochrony Danych Osobowych. Przez okres 5 lat od wdrożenia RODO doktryna wypracowała szereg wytycznych, dobrych praktyk w zakresie stosowania RODO, które powinny być wykorzystywane przez spółki w swojej działalności, tym samym brane pod uwagę podczas przeprowadzania badania DD.

Identyfikacja wymogów mających zastosowanie do badanej spółki powinna zostać przeprowadzona na podstawie ustaleń o których była mowa w drugiej części artykułu, w szczególności dokumentów i informacji udostępnionych w VDR. Jeżeli natomiast badana spółka nie dostarczyła dokumentacji wskazującej na wdrożenie systemu ochrony danych osobowych, dobrą praktyką jest przygotowanie oraz przesłanie listy pytań obejmujących zidentyfikowane obszary mające zastosowanie lub mogące mieć zastosowanie do spółki. Pytania powinny być formułowane w sposób, co do zasady, otwarty – wymagać sporządzenia opisu po stronie odpowiadającego, w celu otrzymania jak największej ilości informacji. Ponadto, powinny dotyczyć dokumentacji jak i odnosić się do procedur związanych ze stosowaniem, reagowaniem oraz monitorowaniem systemu ochrony danych osobowych w organizacji.

Po ustaleniu wszelkich niezbędnych informacji o funkcjonowaniu systemu ochrony danych osobowych, następnym krokiem jest porównanie przyjętych w spółce rozwiązań w zakresie ochrony danych osobowych ze zidentyfikowanymi wcześniej wymogami na gruncie obowiązujących przepisów oraz wytycznych organów.

Należy przy tym pamiętać, że sama dokumentacja nie równa się poprawnemu wdrożeniu i stosowaniu wymogów RODO. Może dochodzić do sytuacji, że dokumentacja jest prowadzona w sposób prawidłowy tj. zgodnie z ogólnymi wymogami, jednakże ze względu na swoją treść nie ma ona pokrycia w faktycznej działalności spółki lub nie została w ogóle wdrożona (nie jest w ogóle uchwalona). O ile drugi problem można rozwiązać poprzez odpowiednie zastrzeżenia w treści raportu z badania DD, o tyle zgodność dokumentacji z faktyczną działalnością spółki wymaga poczynienia dodatkowych ustaleń przez badającego. Prostym sposobem na namierzenie rozbieżności w tym względzie jest szukanie elementów w systemie ochrony danych osobowych które są ze sobą wewnętrznie sprzeczne, jak np.: określenie w polityce ODO obowiązków inspektora ochrony danych („IOD") zw zakresie

realizacji praw podmiotów danych podczas gdy w organizacji nie został powołany IOD. Co więcej, na taki fakt wskazywać może również ujęcie jakiegoś elementu w jednym miejscu, a nie uwzględnienie, nierozwinięcie w innym np.: w treści klauzuli informacyjnej zidentyfikowane są transfery i ich występowanie, ale brak dokumentacji legalizującej (stosowanych SCC, BCR itd.), wytycznych, procedur, analiz z tym związanych.

Jak kwalifikować ryzyka w raporcie z badania DD?

Zidentyfikowane nieprawidłowości powinny zostać w sposób odpowiedni opisane w raporcie z badania DD. W zależności od przyjętej formy badania tj. i. „Full Scope Due Diligence" (FS DD), ii. „Red Flag Due Diligence" (RF DD) zidentyfikowane nieprawidłowości będą opisywane w różny sposób. Raport FS DD będzie zawierał szeroki opis funkcjonowania systemu ochrony danych osobowych wraz ze wszystkimi zidentyfikowanymi nieprawidłowościami oraz elementami wymagającymi naprawy, natomiast raport RF DD będzie zawierał wyłącznie nieprawidłowości ujęte w formie ryzyk wymagających opisania w raporcie zgodnie z ustalonymi kryteriami istotności.

Z uwagi na dużą popularność na rynku raportów RF DD, w szczególności pod kątem analiz systemów ochrony danych osobowych poniżej kilka słów na temat klasyfikacji ryzyk.

Błędy w zakresie wdrażania i stosowania systemów ochrony danych osobowych są, co do zasady, „naprawialne", dlatego nie będą określane w treści raportu jako tzw. Deal Breaker – jako czynnik mogący wpłynąć na zablokowanie transakcji. Oczywiście nie należy tego stosować bezwarunkowo. W przypadku niewdrożenia lub błędnego wdrożenia systemu ochrony danych osobowych np.: w placówkach medycznych czy zakładach ubezpieczeń, gdzie dochodzi do przetwarzania danych szczególnych kategorii na dużą skalę, uchybienia w zakresie ochrony danych osobowych mogą prowadzić, nawet nie tyle do odstąpienia od transakcji, ale przynajmniej do odsunięcia w czasie w celu umożliwienia przeprowadzenia stosownych działań naprawczych.

Jako krytyczne lub istotne mogą być identyfikowane ryzyka w obszarze ochrony danych osobowych związane m. in. z:

- naruszeniami w zakresie realizacji praw podmiotów danych;
- wszczętymi i toczącymi się postępowaniami administracyjnymi lub sądowo administracyjnymi;
- brakiem wdrożenia systemu ochrony danych osobowych w ogóle;
- naruszeniem zasad przetwarzania danych osobowych, w szczególności przetwarzaniem danych bez podstawy prawnej;

Powyższa lista nie ma charakteru zamkniętego. Wynik badania może być różny m. in. z uwagi na charakter działalności badanej spółki lub ustalone progi istotności czy przyjętą kwalifikację ryzyk.

Podsumowanie

Podsumowując, przeprowadzenie oceny systemu ochrony danych osobowych pod kątem zgodności z obowiązującymi przepisami prawa wymaga indywidualnego podejścia do badanej spółki. Nie jest właściwe wypracowanie jednego schematu czy listy kontrolnej jaka powinna być weryfikowana podczas badania DD spółki pod kątem prawidłowego wdrożenia

systemu ochrony danych osobowych. Przedstawiony w artykule model działania wymaga dużego zaangażowania po stronie badającego oraz zrozumienia specyfiki działalności spółki we wszystkich obszarach. Dopiero takie ustalenia pozwolą na rzetelne przeprowadzenie badania oraz przedstawienie ryzyk w raporcie w sposób zgodny z rzeczywistym stanem rzeczy.

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