Warszawa, 15.05.2024 r.

Fuzje i przejęcia – jak przeprowadzić ten proces zgodnie z RODO?

Przeprowadzone w 2019 r. przez Euromoney Thought Leadership Consulting badanie ponad 500 praktyków zajmujących się fuzjami i przejęciami w Europie, na Bliskim Wschodzie i w Afryce (EMEA) wykazało, że ogólne rozporządzenie o ochronie danych (RODO) miało znaczący wpływ na proces fuzji i przejęć wielu organizacji.

55% ankietowanych praktyków zajmujących się fuzjami i przejęciami potwierdziło, że doświadczyło nieudanych negocjacji z powodu obaw o ochronę danych i zgodność z RODO firmy docelowej.

Niezależnie od tego, czy sprzedajesz, czy nabywasz, dokładny audyt ochrony danych jest niezbędny. Nie tylko ogranicza on ryzyka, ale także zapewnia, że zarówno spółki przejmujące, jak i przejmowane przestrzegają zobowiązań prawnych.

Sprzedający powinni posiadać kompleksową dokumentację wszystkich procesów i polityk ochrony danych, która da kupującemu jasny obraz stanu faktycznego, zwiększy zaufanie i pozwoli na sprawny proces due diligence.

Kupujący z kolei powinni dokładnie ocenić praktyki sprzedającego w zakresie ochrony danych i oszacować związane z nimi ryzyka i zobowiązania. Systematyczny przegląd dokumentacji może wyjaśnić wszelkie kwestie, pomóc w podejmowaniu decyzji i ułatwić integrację przetwarzania danych po przejęciu.

Przydatnym narzędziem i punktem wyjścia może być lista kontrolna, które pomoże obu stronom zrozumieć, jakie dokumenty należy uwzględnić, aby wykazać zgodność z przepisami o ochronie danych.

Kluczowa lekcja prywatności - przejęcie hoteli Starwood przez Marriott

W 2016 r. Marriott International przejął Starwood Hotels & Resorts Worldwide, tworząc największą na świecie sieć hoteli. Fuzja zakończyła się sukcesem, ale w 2018 r., niespełna 2 lata po przejęciu, Marriott odkrył naruszenie danych w systemie rezerwacji Starwood.

Naruszenie miało miejsce w 2014 r., ale zostało wykryte dopiero w 2018 r., kiedy wewnętrzne narzędzie bezpieczeństwa wykryło podejrzaną próbę uzyskania dostępu do wewnętrznej bazy danych rezerwacji gości Starwood.

W ramach wewnętrznego dochodzenia Marriott ustalił, że hakerzy zaszyfrowali dane i usunęli je z systemu Starwood. Dane te obejmowały 500 milionów rekordów gości. Informując o naruszeniu, Marriott wskazał, że hakerzy ukradli informacje o gościach, które zawierały „imię i nazwisko, adres pocztowy, numer telefonu, adres e-mail, numer paszportu, informacje o koncie Starwood Preferred Guest ("SPG"), datę urodzenia, płeć, informacje o przyjeździe i wyjeździe, datę rezerwacji i preferencje dotyczące komunikacji. W przypadku niektórych z tych gości skradziono również dane kart płatniczych, ale Marriott nie podał, w przypadku ilu osób".

Ważnym aspektem, na który należy zwrócić uwagę, jest to, że naruszenie trwało przez lata przed wykryciem, co podkreśla istotne niedopatrzenie w procesie due diligence podczas przejęcia.

Brytyjski organ nadzorczy (ICO), który zajmował się ww. incydentem ustalił w toku postępowania wyjaśniającego, że sposób działania hakera był bardzo przebiegły. Zainstalował on w aplikacji systemu sieci Starwood Hotels fragment kodu, który umożliwiał mu zdalny dostęp do informacji zawartych w systemie oraz edycję znajdujących się w nim danych. Jednocześnie, za pośrednictwem złośliwego oprogramowania, zapewnił sobie dostęp do systemu jako użytkownik uprzywilejowany. Jakby tego było mało, haker następnie wdrożył kolejne narzędzia teleinformatyczne, których zadaniem było zgromadzenie wszelkich niezbędnych danych do logowania. W wyniku tych działań, uzyskał on dostęp do bazy danych klientów sieci i wyeksportował ją.

Kara finansowa nałożona przez ICO na Marriott International Inc. robi wrażenie, bo jest to 18 400 000 funtów (niemal 94 000 000 zł)[1].

Warto zauważyć, że postępowanie brytyjskiego regulatora dotyczyło wycieku danych osobowych w związku z cyberatakiem z 2014 r., niemniej administrator został ukarany za nieprawidłowości stwierdzone u niego po 25 maja 2018 r., tj. po dniu, w którym zaczęło obowiązywać RODO.

Należyta staranność i zgodność z RODO

Fuzja Marriott-Starwood miała miejsce przed wejściem w życie RODO. Jest ona jednak wykorzystywana jako przykład tego, co może się stać, jeśli fuzja zostanie przeprowadzona bez dokładnej oceny praktyk w zakresie bezpieczeństwa danych firmy docelowej.

Marriott powinien był przeprowadzić kompleksowy audyt systemów Starwood, procedur przetwarzania danych i środków cyberbezpieczeństwa. Kto wie, może wtedy udałoby się uniknąć tego ogromnego incydentu bezpieczeństwa.

Virtual Data Room

Virtual Data Room (VDR), to przestrzeń online, która jest bezpiecznym miejscem do przechowywania dokumentów podczas procesów biznesowych (fuzje, due diligence, audyty czy postępowania sądowe).

Użytkownicy VDR w przypadku fuzji/przejęć (sprzedający i kupujący) muszą upewnić się, że VDR jest bezpieczny, ponieważ jest to repozytorium, w którym znajdzie swoje miejsce duża ilość wrażliwych i potencjalnie bardzo cennych informacji (nie tylko danych osobowych). Dlatego też pierwszym krokiem powinna być weryfikacja dostawcy VDR w zakresie bezpieczeństwa i ochrony danych.

Ważne jest również, aby w miarę możliwości ograniczyć ilość udostępnianych danych osobowych. Należy rozważyć, co musi zostać udostępnione w ramach procesu due diligence. Istotne dokumenty mogą wymagać anonimizacji lub pseudonimizacji w celu ochrony wrażliwych informacji.

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

Wszelkie obowiązki, zabezpieczenia, wymagane środki techniczne
związane z ochroną danych podczas udostępniania ich do oceny w procesie due diligence muszą zostać uwzględnione w umowie między spółką a dostawcą narzędzia VDR.

Lista kontrolna dotycząca ochrony danych w przypadku fuzji i przejęć

Przedstawiona poniżej lista kontrolna może być punktem wyjścia do przeprowadzenia procesu weryfikacji systemu ochrony danych osobowych podczas przejmowania spółki, ale nie powinna być jej jedynym elementem.

Weryfikacja musi być przeprowadzona z dużym zaangażowaniem osobowym i czasowym. Tylko taka praca pozwoli dokładnie poznać i zrozumieć specyfikę działalności spółki we wszystkich obszarach, a w rezultacie umożliwi rzetelne przeprowadzenie badania oraz przedstawienie ryzyk w raporcie w sposób zgodny z rzeczywistym stanem rzeczy.

Ostatecznie celem jest ustanowienie solidnych podstaw zarządzania ochroną danych, które wykraczają poza transakcję. Zabezpieczy to interesy obu stron i zapewni prawo do prywatności osób, których dane są przetwarzane.

Do podstawowych rejestrów/dokumentów, które trzeba zweryfikować zaliczamy:

1. Rejestr czynności przetwarzania - zapewnia kompleksowy przegląd czynności przetwarzania danych przez organizację i jest obowiązkowym wymogiem zgodnie z art. 30 RODO.
2. Procedury z zakresu realizacji praw osób.
3. Szczegóły dotyczące lokalizacji i przechowywania danych - w tym stosowane środki bezpieczeństwa, które są kluczowym elementem oceny ryzyka związanego z bezpieczeństwem danych.
4. Dokumentację dotyczącą badań wyboru dostawców - wykazuje, że stosowano odpowiednią kontrolę dostawcy w momencie nawiązywania współpracy i w miarę kontynuowania usług.
5. Umowy między administratorem a podmiotami przetwarzającym – pozwalają zrozumieć, z jakimi kontrahentami spółka wymienia dane osobowe i w jakim celu.
6. Oceny prawnie uzasadnionych interesów – weryfikacja uzasadnieniu działań związanych z przetwarzaniem danych w oparciu o prawnie uzasadnione interesy, zgodnie z art. 6 ust. 1 lit. f) RODO.
7. Rejestry naruszeń - prowadzenie dokładnych rejestrów naruszeń ma zasadnicze znaczenie dla zgodności z wymogami RODO w zakresie ochrony danych.
8. Raporty z oceny skutków dla ochrony danych (DPIA) - oceniają ryzyko i wpływ działań związanych z przetwarzaniem danych na prawa i wolności osób fizycznych zgodnie z art. 35 RODO.
9. Wzory klauzul informacyjnych - aktualne informacje zapewniają przejrzystość wobec osób, których dane dotyczą, i odpowiadają wymogom RODO dotyczącym rzetelnego i zgodnego z prawem przetwarzania danych.
10. Rejestry zgód - dokumentują zgodę uzyskaną od osób fizycznych na określone czynności przetwarzania i wykazują zgodność z zasadami określonymi w RODO (w tym z zasadą rozliczalności).

Zainteresowanie tematem danych osobowych podczas fuzji ma kluczowe znaczenie, a kara nałożona przez brytyjskiego regulatora może dać do myślenia wielu przedsiębiorstwom, planującym dokonanie fuzji. Podmioty te powinny bowiem bacznie i ostrożnie przyglądać się systemom teleinformatycznym, które będą nabywać, w szczególności, gdy stanowią one ogromne bazy danych klientów. Jak widać w sprawie dotyczącej sieci Marriott, nigdy nie można wykluczyć ewentualności, że administrator będzie odpowiadać za naruszenia, które są skutkiem różnego typu zdarzeń sprzed wielu lat (i które mogłyby zostać wykryte podczas due diligence), nawet jeżeli nie dotyczą go one bezpośrednio.

Nina Zacharska

Specjalista ds. ochrony danych osobowych