Wdrożenie RODO to dopiero początek drogi

Przepisy ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz dyrektywa NIS to zaledwie początek regulacji, które wymuszą na przedsiębiorcach budowę zintegrowanych systemów ochrony danych osobowych oraz usystematyzowane podejście do bezpieczeństwa nie tylko informacji, lecz także całych sieci i systemów informatycznych.

W myśl badań redakcji „ITwiz" 26,5% polskich przedsiębiorców planuje rozpoczęcie przygotowań do RODO w drugiej połowie 2017 r., 25,3% oczekuje na polskie ustawy z tym związane (zapewne chodzi o tzw. pakiet legislacyjny, ponieważ projekt ustawy dopełniającej RODO został opublikowany w marcu br.), a z kolei 41,3% prowadzi już określone przygotowania.

Konieczność samodzielnej oceny bezpieczeństwa

Powyższe jest o tyle istotne, że zgodnie z przepisami RODO przedsiębiorcy przetwarzający dane osobowe nie będą traktowani jednolicie, jeżeli chodzi o stawiane im wymagania w zakresie zabezpieczeń technicznych. Oznacza to, że nie należy się spodziewać wydania odpowiednika obowiązującego od 2004 r. tzw. rozporządzenia technicznego, które w sposób horyzontalny (tj. dotyczący wszystkich przedsiębiorców) wskazywało na konkretne warunki techniczne i organizacyjne, jakie powinny spełniać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Zamiast tego każdy przedsiębiorca będzie zobowiązany samodzielnie dokonywać oceny w zakresie tego, jakie rozwiązania i technologie pozwolą na zabezpieczenie przetwarzanych przez niego danych w sposób adekwatny do ich kategorii i sposobu wykorzystania. Do takich rozwiązań należy zaliczyć pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, a także regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W myśl przepisów RODO przedsiębiorcy przetwarzający dane osobowe nie będą traktowani jednolicie, jeżeli chodzi o stawiane im wymagania w zakresie zabezpieczeń technicznych. Oznacza to, że nie należy się spodziewać wydania odpowiednika obowiązującego od 2004 r. tzw. rozporządzenia technicznego, które w sposób horyzontalny (tj. dotyczący wszystkich przedsiębiorców) wskazywało na konkretne warunki techniczne i organizacyjne, jakie powinny spełniać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Dodatkowo część przedsiębiorców została wymieniona wprost w dyrektywie NIS, np. przedsiębiorstwa energetyczne, które są dostawcami, operatorzy systemów przesyłowych oraz dystrybucyjnych, a także przedsiębiorstwa dostarczające gaz i dostawcy usług przetwarzania w chmurze. Tym samym mają oni zostać zobowiązani do podejmowania: (a) odpowiednich i proporcjonalnych środków w celu zarządzania ryzykiem oraz (b) odpowiednich środków zapobiegających incydentom zagrażającym bezpieczeństwu komputerowemu i minimalizujących wpływ tych, które już wystąpiły, a także niezwłocznego zgłaszania właściwemu organowi lub CSIRT (zespołowi ds. reagowania) incydentów mogących nieść istotne zagrożenie. Należy zwrócić uwagę, że powyższe obowiązki dotyczą wykorzystywanych przez tych przedsiębiorców systemów i sieci niezależnie od tego, czy służą one do przetwarzania danych osobowych.

W dyrektywie NIS wymienione zostały wprost przedsiębiorstwa energetyczne, które są dostawcami, operatorzy systemów przesyłowych oraz dystrybucyjnych, a także przedsiębiorstwa dostarczające gaz i **dostawcy usług przetwarzania w chmurze. Tym samym mają oni zostać zobowiązani do podejmowania: (a) odpowiednich i proporcjonalnych środków w celu zarządzania ryzykiem oraz (b) odpowiednich środków zapobiegających incydentom zagrażającym bezpieczeństwu komputerowemu i minimalizujących wpływ tych, które już wystąpiły, a także niezwłocznego zgłaszania właściwemu organowi lub CSIRT (zespołowi ds. reagowania) incydentów mogących nieść istotne zagrożenie.**

Normy wspierające dostosowanie do RODO

Podczas realizacji przedstawionych powyżej wymagań przydatne będą określone normy i standardy (np. ISO 27001, CSA CCM, BSI C5, COBIT 5, TOGAF, CCS, OCF, NIST), zalecenia raportów Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (np. raport Prywatność i ochrona danych w fazie projektowania – od polityki do inżynierii), a w przyszłości zatwierdzone przez odpowiednie organy kodeksy dobrych praktyk, akredytowane mechanizmy certyfikowania/znaków jakości, a także zalecenia Europejskiej Rady Ochrony Danych Osobowych (dzisiejsza Grupa Robocza Art. 29). Nie bez znaczenia mogą być również dobre praktyki ładu korporacyjnego publikowane przez Giełdę Papierów Wartościowych.

Co istotne, jest bardzo prawdopodobne, że w przypadku określonych grup przedsiębiorców wymienione powyżej obowiązki i tak mogą okazać się dla unijnego prawodawcy niewystarczające. Przykładowo, w marcu 2017 r. grupa ekspercka Komisji Europejskiej EECSP (Energy Expert Cyber Security Platform) opracowała obszerny raport dotyczący cyberbezpieczeństwa w sektorze energetycznym. Celem raportu było dokonanie oceny obecnych regulacji dotyczących tego obszaru w kontekście usług energetycznych, a także wskazanie działań, jakie powinno się podjąć dla podniesienia poziomu ochrony systemów i przetwarzanych w ich ramach informacji.

EECSP zidentyfikowała 10 kluczowych obszarów z zakresu cyberbezpieczeństwa w energetyce, w ramach których wskazała 39 luk prawnych, jakie powinny zostać uzupełnione w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Co ciekawe, doszło do tego w sytuacji, gdy większość polskich przedsiębiorców energetycznych dopiero rozpoczęła proces dostosowywania własnej organizacji do przepisów RODO oraz oczekuje na projekt krajowej ustawy o cyberbezpieczeństwie, która ma za zadanie implementować do krajowego porządku prawnego przepisy dyrektywy NIS.

Za uzasadnione należy zatem uznać stwierdzenie, że nawet po dostosowaniu się przedsiębiorców energetycznych do obu ww. regulacji będą ich czekać kolejne zmiany m.in. w zakresie powyższych zidentyfikowanych przez EECSP luk prawnych. Do ww. luk zaliczono np. brak przyjęcia przez prawodawcę unijnego wspólnych dla sektora energetycznego kryteriów zgłaszania incydentów bezpieczeństwa komputerowego.

Jednocześnie należy pamiętać o tym, że wciąż toczą się prace nad nowym rozporządzeniem o prywatności i łączności elektronicznej. Nowych regulacji będzie zatem tylko przybywać, a przedsiębiorcy powinni na stałe wmontować kompetencje w zakresie ochrony informacji i systemów do struktury swojej organizacji.

Paweł Gruszecki,
radca prawny, partner, szef Praktyki Nowych Technologii i Telekomunikacji, Kochański Zięba & Partners