RODO – poważne zmiany dla sklepów internetowych

Choć do wejścia w życie nowych przepisów dotyczących ochrony danych osobowych i obowiązku implementacji rozwiązań z zakresu data protection pozostało jeszcze blisko 9 miesięcy, to dla wielu właścicieli sklepów internetowych jest to już ostatni dzwonek na rozpoczęcie wdrażania procedur zgodności z RODO

Polska # KPRF Law Office

TEKST:
ADWOKAT **ANNA ZEJDLER**,
KPRF LAW OFFICE

fot. KPRF Law Office, Shutterstock

Przepisy RODO zawierają szerszą regulację dotyczącą umów powierzenia przetwarzania danych osobowych

K | P | R | F
LAW OFFICE

Audyty bezpieczeństwa, konieczność dostosowania procesów biznesowych i systemów informatycznych, a także szkolenia pracowników mogą potrwać wiele miesięcy, a czasu coraz mniej. Zmiany dotkną tak naprawdę wszystkie firmy, które gromadzą i wykorzystują dane osobowe dotyczące osób fizycznych – duże międzynarodowe sieci, sklepy oferujące karty stałego klienta, sklepy internetowe i wszystkie inne formy działalności, które posiadają dostęp do danych osobowych swoich klientów. Co niesie ze sobą wejście RODO, w jaki sposób przygotować się do jego wejścia w życie i na jakie aspekty funkcjonowania przedsiębiorstwa zwrócić uwagę, skoro zostało tak mało czasu?

W dniu 25 maja 2018 roku wejdzie w życie Rozporządzenie ogólne o ochronie danych osobowych, Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (dalej jako RODO), które zastąpi dotychczas obowiązującą dyrektywę 95/46/WE, a które z uwagi na jego jednolite i bezpośrednie stosowanie w Unii Europejskiej zastąpi również polską ustawę o ochronie danych osobowych. Do tego czasu podmioty zobowiązane do stosowania rozporządzenia, przede wszystkim przedsiębiorcy, będą musiały dostosować się i wdrożyć wytyczne unijnego rozporządzenia, zagadnienie ochrony danych przejdzie zaś na inny, znacznie wyższy poziom ryzyka, a jednocześnie zmierzy się ze zmieniającą się rzeczywistością.

Brak wdrożenia RODO i niestosowanie się do wprowadzonych przepisów może oznaczać dla przedsiębiorców odpowiedzialność finansową w postaci kar administracyjnych w wysokości do 20 mln euro bądź do 4 proc. całkowitego rocznego obrotu z poprzedniego roku obrotowego oraz możliwość dochodzenia roszczeń na drodze cywilnej w związku z naruszeniem nowych przepisów wobec osób, których dane są przetwarzane.

DOKUMENTACJA WEWNĘTRZNA, OBOWIĄZEK INFORMACYJNY I ZGODY

Zgodnie z RODO administrator danych osobowych (dalej jako „ADO") powinien wdrożyć odpowiednie środki techniczne i organizacyjne, uwzględniające charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko z nim związane, co w praktyce wiązać się będzie z opracowaniem dokumentacji opisującej procedury i procesy bezpiecznego przetwarzania danych osobowych w firmie oraz aktualizacją uprzednio obowiązujących procedur ochrony danych, w tym dokonania ich przeglądu, uzupełnienia lub dostosowania.

Klauzule informacyjne stosowane dotychczas w standardowych politykach prywatności obejmowały wąski zakres informacji i ograniczały się do obowiązku wskazania nazwy i adresu siedziby ADO, określenia celu przetwarzania danych, określenia odbiorców, którym dane są udostępniane, poinformowania o obowiązkowym lub dobrowolnym charakterze zbierania danych oraz wskazania przysługujących uprawnień. RODO rozszerzyło dotychczasowy katalog i nałożyło na ADO nowe obowiązki informacyjne, dotyczące w szczególności (i) okresu przechowywania danych osobowych lub kryteriów ustalania jego długości, (ii) informacji o prawie cofnięcia zgody na przetwarzanie danych osobowych, prawie ich sprostowania, usunięcia, ograniczenia przetwarzania, (iii) informacji o prawie sprzeciwu wobec przetwarzania danych oraz prawie do ich przenoszenia, (iv) informacji o prawie wniesienia skargi, (v) informacji o ewentualnym profilowaniu danych, (vi) danych kontaktowych do Inspektora Ochrony Danych, o ile został powołany. W konsekwencji, od dnia wejścia w życie RODO, każdy ADO powinien stosować nowe polityki prywatności oraz nowe klauzule informacyjne w umowach, regulaminach czy formularzach.

REJESTR CZYNNOŚCI PRZETWARZANIA

RODO nakłada na ADO nowy obowiązek w zakresie prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiadają, który to rejestr powinien być prowadzony w formie pisemnej (papierowej lub elektronicznej). Prowadzony rejestr będzie musiał obejmować informacje dotyczące m.in. celu przetwarzania danych, kategorii danych osobowych, kategorii odbiorców danych oraz technicznych i organizacyjnych środków zabezpieczenia danych. Powyższy obowiązek nie będzie dotyczył jedynie tych podmiotów, które zatrudniają mniej niż 250 osób, ale tylko wtedy, gdy przetwarzanie przez nie danych osobowych ma charakter sporadyczny, nie powoduje ryzyka naruszenia praw i wolności osób, których dane dotyczą, oraz nie obejmuje danych wrażliwych.

Brak wdrożenia RODO i niestosowanie się do wprowadzonych przepisów może oznaczać dla przedsiębiorców odpowiedzialność finansową

KORZYSTANIE Z PODWYKONAWCÓW I UMOWY POWIERZENIA

Kolejną istotną kwestią w świetle RODO jest korzystanie z podwykonawców i powierzenie przetwarzania danych osobowych podmiotom trzecim, co w praktyce może dotyczyć np. usług hostingu czy outsourcingu usług na podmioty zewnętrzne.

Przepisy RODO zawierają szerszą regulację dotyczącą umów powierzenia przetwarzania danych osobowych, w tym wymagają m.in. aby umowa powierzenia określała nie tylko cel i zakres powierzonego przetwarzania, lecz również rodzaj danych, kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora. W praktyce oznacza to konieczność analizy, jakie umowy dotyczące powierzenia przetwarzania danych zostały zawarte i z kim, oraz ich aneksowania tak, aby ich treść odpowiadała nowym wymogom RODO. Jeżeli z jakiegoś powodu nie zostały uprzednio zawarte umowy z podmiotami, którym zostało zlecone przetwarzanie danych osobowych, okres przejściowy przed obowiązywaniem RODO to ostatni moment na naprawienie tych braków. W przypadku niewprowadzenia odpowiednich zapisów do umów powierzenia i niezabezpieczenia sposobu przetwarzania danych pełną odpowiedzialność za działanie podmiotu przetwarzającego dane osobowe ponosić będzie ADO.

INFORMOWANIE O NARUSZENIACH

RODO nakłada na ADO obowiązek zgłaszania naruszeń danych osobowych (np. w wyniku wycieku danych osobowych) do organu nadzoru niezwłocznie, jednak nie później niż w terminie 72 godzin od momentu wykrycia takiego naruszenia. Co więcej, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki powinien zawiadomić osobę, której dane dotyczą, o takim naruszeniu. Pamiętać przy tym należy, że dokonanie zgłoszenia nie będzie jedynie dobrą wolą przedsiębiorcy, tylko jego ustawowym obowiązkiem, którego niedotrzymanie może być sankcjonowane nawet na drodze postępowania karnego.