https://doi.org/10.26881/sim.2017.4.08

Olga Dębicka
Adam Borodo
Jacek Winiarski

OCHRONA DANYCH OSOBOWYCH W BRANŻY E-COMMERCE W POLSCE

STRESZCZENIE

W dniu 25 maja 2018 roku wchodzi w życie rozporządzenie Parlamentu Europejskiego i Rady UE 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. Rozporządzenie to będzie stosowane jednolicie i bezpośrednio w całej Unii Europejskiej, obligując tym samym przedsiębiorców działających w Polsce, w tym w obszarze e-commerce, do dostosowania się do nowych regulacji.

W artykule dokonano analizy wyzwań oraz konsekwencji, jakie wnosi zmiana przepisów w zakresie ochrony danych osobowych do branży e-commerce, pokazując tym samym, w jaki sposób przepisy rozporządzenia wpłyną na świadczenie usług drogą elektroniczną. W artykule uwzględniono główne obszary zmian, w tym modyfikację konstrukcji zgody na przetwarzanie danych, zwiększenie kontroli nad danymi osobowymi, informowanie o naruszeniach ochrony danych oraz warunki dopuszczalności przekazywania danych do państwa trzeciego. W tym celu wykorzystano badania literaturowe oraz metodę intuicyjną. Przeprowadzono również pilotażowe badania wśród przedsiębiorców świadczących usługi e-commerce w województwie pomorskim, posługując się przy tym metodą wywiadu pogłębionego w modelu CATI (*Computer-Assisted Telephone Interview*) oraz poprzez pojedynczy mailing CAWI (*Computer-Assisted Web Interview*).

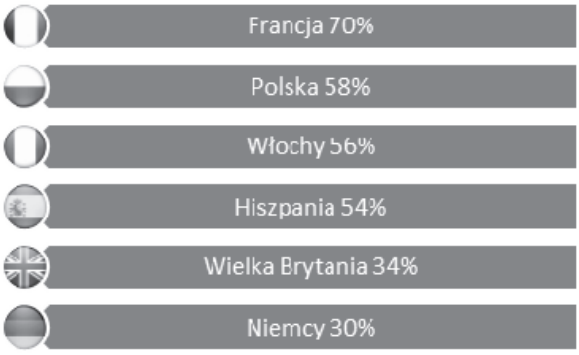
Słowa kluczowe: ochrona danych osobowych, e-commerce.

Wstęp

Prowadzenie działalności handlowej w Internecie wiąże się z koniecznością zwracania szczególnej uwagi przez przedsiębiorców na zagrożenia pochodzące z sieci, w tym szczególnie na ochronę poufnych informacji finansowych i danych osobowych przy składaniu zamówienia przez formularz czy dokonywaniu płatności online. Naruszenie prawa ochrony danych osobowych może przybrać różną postać, poprzez np.: niezgłoszenie zbioru danych osobowych do rejestru prowadzonego przez Głównego Inspektora Danych Osobowych (dalej: GIODO), niewłaściwe zabezpieczenie danych osobowych, nieupoważnione udostępnienie danych osobowych osobom trzecim, przetwarzanie danych osobowych w zbiorze mimo niedopuszczalności takiej działalności.

Przedsiębiorstwa e-commerce, które gromadzą i przetwarzają informacje teleadresowe klientów, oprócz obowiązku zgłoszenia zbioru danych osobowych, muszą go zatem odpowiednio zabezpieczyć.

Konieczne jest stworzenie tzw. polityki bezpieczeństwa, czyli dokumentu opisującego reguły, procedury oraz procesy stosowane w celu ochrony danych wrażliwych. W Polsce, w celu spełnienia wymogu w zakresie ochrony danych osobowych, należy np. stosować szyfrowanie SSL w formularzach, za pośrednictwem których przesyłane są dane osobowe. Ta metoda jest obecnie już standardem, a jej użycie wpływa pozytywnie na wizerunek przedsiębiorstwa, które ją stosuje. Zwiększa to zaufanie klientów, stąd wiele sklepów informuje o szyfrowaniu adresu URL za pomocą informacji podanych na stronie głównej swojego sklepu. Tego typu praktyka ma miejsce najczęściej w sklepach internetowych we Francji, gdzie aż 70% sprzedawców w bezpośredni sposób informuje o tym fakcie swoich użytkowników (rysunek 1).



Rysunek 1. Informacje o szyfrowaniu danych w e-sklepach (udział sprzedawców informujących na stronie głównej swojego sklepu o szyfrowaniu danych za pomocą protokołu SSL)

Źródło: [Podjacki, 2016].

Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO) z 27 kwietnia 2016 roku, wydane przez Parlament Europejski i Radę UE, zwraca uwagę właśnie na zagrożenia związane z nowymi technologiami, stosowanymi m.in.

w e-commerce. Kładzie ono nacisk na dokonanie oceny skutków przetwarzania danych osobowych w procesie planowania prowadzenia działalności gospodarczej. Zobowiązuje każdego przedsiębiorcę, jako administratora danych, do przeanalizowania wpływu działalności na ochronę danych osobowych, które przedsiębiorca zamierza przetwarzać.

Dla podmiotów prowadzących e-handel nowe rozporządzenie wprowadza daleko idące zmiany w zakresie ochrony danych osobowych.

1. Prywatność i zaufanie w e-handlu

Zarówno kwestie etyczne, jak i związane z nimi akty prawne muszą zostać uwzględnione przez przedsiębiorców, stanowią one część otoczenia biznesowego. Jedną z niezwykle istotnych kwestii w e-handlu jest prawo do prywatności, które uznaje się jako prawo człowieka pierwszej generacji (wg. K. Vasaka, który pod koniec lat 70. XX w. zaproponował podział praw człowieka na trzy generacje), zaś ochrona sfery życia prywatnego zaliczana jest przez akty międzynarodowe dotyczące praw człowieka do katalogu praw fundamentalnych, a zatem chronionych. Prawo do ochrony prywatności zagwarantowane jest zarówno w prawie międzynarodowym (Konwencja o ochronie praw człowieka i podstawowych wolności: *„Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji*" (art. 8)), prawie europejskim oraz w polskim systemie prawnym – Konstytucja RP z 1997 r.: *„Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym*" (art. 47) [Pryciak, 2010].

Prywatność stanowi również przedmiot troski osób dokonujących transakcji w sieci, stając się tym samym kluczowym zagadnieniem etycznym wywierającym wpływ na e-handel. Determinuje ona bowiem zaufanie klientów przekładające się na podejmowanie decyzji zakupowych. Kwestia prywatności w zakresie danych osobowych, zarówno zapobiegająca wtargnięciu w sferę osobistą jednostki przez osoby trzecie, jak i zapewniająca ich bezpieczeństwo, w tym przed coraz częstszymi kradzieżami tożsamości, stanowi coraz poważniejszy problem zarówno dla e-klientów, jak i dla firm prowadzących sprzedaż w internecie.

Problemy etyczne związane z własnością informacji osobistych, a tym samym z prywatnością klientów, rozpatrywać można w trzech obszarach odnoszących się zarówno do klientów jak i sprzedawców [Fletcher, 2001]:

- **transparentności,** mówiącej o podmiocie gromadzącym informacje, rodzaju gromadzonych informacji, sposobie ujawniania faktu ich gromadzenia i celu ich wykorzystania;
- **bezpieczeństwa,** odnoszącego się do sposobu ochrony informacji po ich uzyskaniu przez przedsiębiorstwo;
- **odpowiedzialności prawnej,** mówiącej o tym, kto ponosi odpowiedzialność w przypadku niewłaściwego użytkowania danych.

Prywatność klienta w e-handlu wiąże się z dwoma podstawowymi problemami, tj. zabezpieczeniem przed kradzieżą tożsamości oraz ograniczeniem przesyłania niepożądanych wiadomości e-mail (zwykle wysyłanych grupowo i nienakierowanych na konkretną grupę docelową). Obawy klientów stoją niejako w opozycji do potrzeb informacyjnych przedsiębiorców, którym gromadzenie informacji o klientach pozwala na zrozumienie ich potrzeb i zachowań, umożliwiając tym samym stworzenie bardziej spersonalizowanej i ukierunkowanej oferty, co sprzyja wzrostowi sprzedaży (tabela 1).

Tabela 1. Technologie wykorzystywane do zbierania informacji w sieci wg. grup potrzeb informacyjnych w e-handlu

Rodzaj informacji	Technologie wykorzystywane do gromadzenia i wykorzystywania informacji
Informacje kontaktowe	– formularze elektroniczne – zintegrowane z bazami danych klientów, – pliki cookie – zapamiętujące kolejne odwiedziny danego klienta
Informacje profilowe (także prywatne)	– formularze rejestracyjne online zbierające dane na stronach sklepów, – wykorzystanie plików cookie do przyporządkowania klienta do danego segmentu (pobrane z bazy danych) i wyświetlenie zawartości dopasowanej do tego segmentu
Obsługa platformy dostępowej	– systemy analityki sieciowej (identyfikacja komputera, systemu operacyjnego na podstawie atrybutu http klienta)
Informacje o typowych zachowaniach w pojedynczej witrynie	– historie zakupów gromadzone w bazie danych zamówień, – znacznik web beacon używany do stwierdzenia czy użytkownik otworzył e-maila (wykorzystywane w marketingu e-mailowym), – pliki cookie wykorzystywane do monitorowania zachowania na pojedynczej witrynie
Informacje o zachowaniach w wielu witrynach	– pliki cookie podmiotów zewnętrznych używane do analizowania wizyt przekierowanych z innych witryn, – korzystanie z plików cookie przez wyszukiwarki (Google) do śledzenia reakcji na reklamy AdWords, – monitorowanie ruchu IP w celu dokonania oceny użytkowania witryny przez grupy klientów w ramach określonej kategorii produktów.

Źródło: [Chaffey, 2016, s. 144].

Potrzeby informacyjne przedsiębiorców dotyczą pięciu głównych obszarów:

1. **informacji kontaktowych,** tj. nazwiska, adresu i maila klienta,
2. **informacji profilowych** odnoszących się do wieku, płci, grupy społecznej, pozwalających na dokonanie segmentacji klientów,
3. **danych z zakresu użytkowania platformy**, w tym rodzaju komputera, przeglądarki czy rozdzielczości ekranu użytkowników strony,
4. **informacji o zachowaniach w pojedynczej witrynie,** dotyczące procesu dokonywania zakupu czy historii zakupów,

5. **informacji o zachowaniach w wielu witrynach,** gromadzone poprzez wykorzystanie profili opartych na adresach IP czy plikach cookie, pozwalających na jednoznaczną identyfikacje użytkownika [Chaffey, 2016].

Dokonywanie zakupów w sklepie internetowym wiąże się dla klientów z przekazywaniem swoich poufnych danych, które zakwalifikować można do dwóch pierwszych obszarów wymienionych powyżej. Istotnym zagadnieniem w e-handlu, które wpływa na budowanie zaufania jest zapewnienie właściwego bezpieczeństwa dokonywanych transakcji, tak by klienci mogli bez ryzyka przekazywać te dane czy dokonywać płatności. Wymaga to od sprzedawców właściwego podejścia i dokonania wszelkich starań, by podawane przez klientów informacje były w odpowiedni sposób chronione. Jest to bowiem jeden z niezbędnych elementów budowy zaufania klientów, które zdaniem P. Kosseckiego jest niezbędne do tego, by klient udostępniał swoje dane osobowe, w celu dokonania zakupów online bez bezpośredniego kontaktu ze sprzedawcą [Kossecki, 2009]. Działania podejmowane w tym zakresie przez e-sprzedawców mogą dotyczyć zarówno budowy zaufania wykalkulowanego, osobistego ale również instytucjonalnego, które opiera się na obowiązujących regulacjach prawnych [Grudzewski, 2009].

2. Akty prawne odnoszące się do ochrony danych osobowych w e-handlu

Obowiązek ochrony przetwarzanych danych osobowych ciąży na każdym właścicielu e-sklepu czy serwisu internetowego, który taki zbiór danych gromadzi. W Unii Europejskiej kwestie ochrony danych osobowych objęte są przepisami zawartymi w Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.

Rada Europy określiła w niej nie tylko podstawowe standardy ochrony danych osobowych, ale również rekomendacje, które stały się podwalinami do opracowania regulacji prawnych w krajach członkowskich UE. W Dyrektywie podkreślono, iż człowiek ma prawo być anonimowym, tzn. może decydować o informacjach jakie mogą być o nim udostępnione osobom trzecim. Powinien on również posiadać prawo „dostępu do danych określających szeroko rozumianą tożsamość oraz uprawnienia do ich poprawiania i usuwania, gdyby informacje te były w posiadaniu niepowołanych do tego podmiotów" [Pryciak, 2010].

Obowiązujące w Dyrektywie 95/46/WE przepisy o ochronie danych osobowych do polskiego porządku prawnego wprowadziła Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r (tekst jedn. Dz.U. z 2015 r. poz. 2135 z późn. zm.). Zagadnienia te również regulowane są w Kodeksie karnym i Konstytucji RP.

Głównym celem Dyrektywy 95/46/WE była harmonizacja przepisów dotyczących ochrony danych osobowych w poszczególnych państwach członkowskich UE oraz wprowadzenie podstawowego standardu w zakresie ich ochrony

[Ożgalska-Trybalska, 2001]. Dyrektywa ta definiuje kluczowe z perspektywy e-handlu terminy takie jak dane osobowe, przetwarzanie danych osobowych, zbiór danych, osoba trzecia, odbierający dane czy też zgoda osoby, której dane dotyczą [Dyrektywa 95/46/WE, art. 2]. W Dyrektywie dostrzeżono również konieczność uwzględnienia transgranicznego przepływu danych osobowych, istotnego przy sprzedaży *cross-border* w e-handlu. Dyrektywa dopuszcza również udostępnianie danych osobowych do państw trzecich, jeśli państwa te zapewniają odpowiedni poziom ochrony, zaś w przypadku jego braku przekazanie danych osobowych jest możliwe tylko wówczas, gdy osoba, której dane dotyczą, wyrazi na to zgodę [Dyrektywa 95/46/WE, s. 58].

Z uwagi na to jednak, że przepisy dotyczące ochrony danych osobowych zawarte w Dyrektywie pochodzą z 1995 roku, tym samym nie uwzględniają zmian wywołanych przez wzrost wykorzystania internetu, rozwój handlu elektronicznego, portali społecznościowych czy usług cloud computingu, konieczne stało się jej dostosowanie do zmieniającej się rzeczywistości gospodarki cyfrowej.

Prace nad reformą systemu ochrony danych osobowych w Unii Europejskiej rozpoczęły się w styczniu 2012 roku, zaś ich celem było opracowanie nowego projektu Rozporządzenia ogólnego o ochronie danych osobowych (RODO) zmieniającego Dyrektywę 95/46/WE poprzez zapewnienie solidnych i spójnych ram prawnych dotyczących wszystkich obszarów polityki UE, ograniczenie obciążeń administracyjnych dla przedsiębiorców oraz wzmocnienie praw osób fizycznych [Grzelak, 2015]. *General Data Protection Regulation* (GDPR), czyli Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO) było opracowywane i dyskutowane przez cztery lata, a ostatecznie przyjęte zostało przez Parlament Europejski i Radę Unii Europejskiej w kwietniu 2016 r., obowiązywać zaś będzie od 25 maja 2018 r.

Zwiększenie przez UE bezpieczeństwa danych obliguje przedsiębiorstwa i organizacje do adekwatnej ochrony wrażliwych danych osobistych, zdefiniowanych jako: „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą)"; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4 ust. 1 RODO).

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 jest aktem prawnym, który nie tylko dostosowuje wymogi ochrony danych osobowych do zmian zachodzących w światowej gospodarce, ale jest aktem, który wymusza na przedsiębiorstwach zmianę podejścia do całego systemu ochrony danych osobowych. Ta zmiana stanowi wyzwanie zarówno technologiczne jak również mentalne i organizacyjne.

Najważniejsze zmiany wprowadzane przez projekt nowego Rozporządzenia o ochronie danych osobowych, w stosunku do obecnie obowiązującej Dyrektywy, dotyczą m.in.:

- wprowadzenia instytucji certyfikacji wraz ze znakami jakości i oznaczeniami oraz w mniejszym stopniu kodeksów postępowania,
- notyfikacji, profilowania, prawa do bycia zapomnianym,
- uprawnienia do przeniesienia danych i wiele innych rozwiązań, niespotykanych do tej pory w systemach ochrony danych, ale nie ujętych w konkretne ramy prawne,
- nowych dokumentów i mechanizmów kontroli nad danymi.

3. Konsekwencje zmian w RODO dla sklepów internetowych

Konsekwencją wprowadzenia RODO będzie wzrost znaczenia reguł przetwarzania danych osobowych w codziennej praktyce przedsiębiorców. Wynika to z diametralnej zmiany podejścia regulacyjnego do sankcji administracyjnych z tytułu naruszenia zasad przetwarzania danych, skutkującej znaczącym zaostrzeniem odpowiedzialności administratorów i innych podmiotów dokonujących operacji na zbiorach danych osobowych. Sankcje proponowane przez RODO są znacząco większe niż do tej pory obowiązujące w polskim ustawodawstwie.

Dotychczasowy kształt regulacji obowiązujących w Polsce przewidywał możliwość nałożenia przez GIODO grzywny w wysokości maksymalnie 10 000 zł w stosunku do osoby fizycznej lub 50 000 zł w stosunku do osoby prawnej, a łączna wysokość kar (nakładanych wielokrotnie) nie mogła przekroczyć odpowiednio 50 000 zł i 200 000 zł, przy czym nałożenie grzywny mogło nastąpić dopiero po niedostosowaniu się przez przedsiębiorstwo do decyzji GIODO nakazującej usunięcie naruszeń stwierdzonych w toku kontroli, w zakresie zgodności przetwarzania danych.

Niedopilnowanie nowych obowiązków dotyczących ochrony danych osobowych może z kolei skutkować nałożeniem kary wynoszącej odpowiednio do 10 mln euro lub 2% rocznego obrotu przedsiębiorstwa (art. 73 ust. 3-3aa RODO) oraz kary do 20 mln euro lub 4% rocznego obrotu (art. 79 ust. 3a RODO). Sankcja pierwsza odnosi się do naruszenia technologicznego i organizacyjnego zasad przetwarzania danych, w tym wdrożenia odpowiednich środków ochrony danych osobowych, odpowiedzialności za rozwiązania stosowane przez tzw. podmiot przetwarzający (w ramach powierzenia przetwarzania danych), czy też do braku zgłoszenia przypadków naruszenia bezpieczeństwa danych osobowych [Koellner, 2017].

Kary do 20 mln euro lub 4% rocznego obrotu przedsiębiorstw przewidziane są w RODO za naruszenie podstawowych zasad postępowania z danymi osobowymi, w tym w szczególności podstaw prawnych przetwarzania danych osobowych, tj. zasady lub minimalizacji przetwarzania danych, zasady związania

celem przetwarzania, zasady transparentności przetwarzania, a w szczególności podstaw prawnych przetwarzania danych osobowych.

Podmioty działające w branży e-commerce muszą się zatem dobrze przygotować do wprowadzenia odpowiednich polityk bezpieczeństwa oraz instrukcji, a także dogłębnego przeszkolenia swoich pracowników i współpracowników. Naruszanie prawa przestanie być bowiem bezkarne, a obowiązkiem (GIODO) nałożonym przez prawodawcę unijnego będzie doprowadzenie do stanu, w którym polscy przedsiębiorcy będą dochowywali obowiązków określonych w prawie ochrony danych osobowych. Narzędziem dla tego celu mają być między innymi opisane wcześniej sankcje.

W praktyce e-handlu nowe regulacje oddziałują w szczególny sposób na zasady zbierania danych osobowych i zgody na ich przetwarzanie, a więc na dotychczasową praktykę stosowania „checkbox'ów" oraz na bardzo istotne w handlu internetowym profilowanie klientów, które jest kluczem w budowaniu sieci odbiorców usług lub towarów.

Zgodnie z art. 21 ust 1 i 2 „Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów". Co więcej, zgodnie z ust. 2 tego artykułu „Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu (w tym profilowania) w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim".

W związku z powyższym, przedsiębiorstwa e-commerce, które będą chciały stosować w swojej działalności profilowanie, obowiązane są na gruncie nowego rozporządzenia do spełnienia – oprócz obowiązków wspólnych dla wszystkich przetwarzających dane – dodatkowych wymogów zarezerwowanych dla tej formy przetwarzania. Obowiązkiem administratora danych, który profiluje (lub zamierza profilować) jest przede wszystkim poinformowanie o tym fakcie osób fizycznych objętych profilowaniem. Co więcej, administrator zobowiązany jest poinformować o zasadach profilowania, jego znaczeniu oraz przewidywanych konsekwencjach dla jednostek. Obowiązek ten uniemożliwia lub znacząco ogranicza profilowanie użytkowników w sposób ukryty [Pękała, 2017]. Związane jest to bezpośrednio z tzw. obowiązkiem informacyjnym, który oznacza, iż każdej osobie, której dane dotyczą, przedsiębiorca jest zobowiązany podać informacje o profilowaniu oraz o prawach do sprzeciwu lub niepodlegania decyzjom podjętym w wyniku profilowania. Obowiązek ten przedsiębiorca może spełnić poprzez informację pod formularzem zamówienia lub informację drogą mailową.

Kolejną ważną kwestią dla e-sklepów będzie zapewnienie klientom prawa do bycia zapomnianym, które stanowi, iż każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo osoby, której dane dotyczą, do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane. Klient e-sklepu będzie miał prawo żądania od administratora

niezwłocznego usunięcia jego danych osobowych, a administrator będzie miał obowiązek bez zbędnej zwłoki usunąć te dane, jeśli klient cofnie zgodę na ich przetwarzanie, jeśli wniesie sprzeciw wobec przetwarzania tych danych, jeśli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane lub jeśli przetwarzanie danych osobowych nie jest z innego powodu zgodne z rozporządzeniem ogólnym (art. 17 ust. 1 rozporządzenia ogólnego).

Dla administratora prawo to oznacza konieczność usunięcia z systemu danych osób, które chciałyby zostać „zapomniane". Co więcej, jeśli dane zostały opublikowane, np. w Internecie, to administrator powinien upewnić się, że wszystkie linki do tych informacji także zostały skasowane, a kopie i repliki pousuwane, nawet jeżeli są w posiadaniu innych podmiotów przetwarzających te dane w imieniu administratora. Ponadto klienci, których dane dotyczą, będą mieli prawo żądania od administratora niezwłocznego sprostowania dotyczących ich danych osobowych, które są nieprawidłowe, a także uzupełnienia niekompletnych danych osobowych [Zawadzka, 2016].

Zmianą, która będzie miała istotny wpływ na prowadzenie e-handlu, jest wprowadzenie przez RODO tzw. zasady rozliczalności. Zasada ta nakłada na administratora (np. przedsiębiorcę prowadzącego sklep internetowy) obowiązek wdrożenia i przestrzegania odpowiednich i skutecznych środków, w celu zapewnienia, że przestrzegane są obowiązki prawne w zakresie ochrony danych. Wymaga ona również, aby przedsiębiorca był w stanie wykazać wypełnienie tego obowiązku. Zastosowane przy tym mogą zostać takie instrumenty, jak: opracowana polityka prywatności, procedury i inna dokumentacja, program szkoleń dla pracowników, audyty zewnętrzne lub wewnętrzne, przeglądy zgodności, certyfikaty itd. W obszarze e-commerce analizie trzeba będzie poddać również wybór podwykonawców, np. świadczących usługi hostingowe czy outsourcing procesów kadrowych, co w praktyce jest normalnym procesem biznesowym. Analiza taka powinna zostać przeprowadzona pod kątem zbadania konieczności aneksowania tych umów gdyż ustawodawca unijny wprowadził szereg dodatkowych elementów, jakie muszą się w nich znaleźć. Ponadto administrator danych powinien sporządzić dokumentację, z której wynika dlaczego tak istotne informacje jak dane osobowe powierzył konkretnemu podmiotowi.

Przy prowadzeniu działalności e-commerce wykraczającej poza granice jednego państwa istotne będą również przepisy dotyczące przetwarzania danych osobowych w kontekście transgranicznym. Jednym z założeń unijnej reformy ochrony danych osobowych było wprowadzenie ułatwień dla tych podmiotów, przede wszystkim jednolitych przepisów oraz mechanizmu określanego mianem „punktu kompleksowej współpracy". Oznacza to konieczność wskazania tak zwanego wiodącego organu nadzorczego, jeśli przetwarzanie danych odbywa się w ramach działalności jednostek organizacyjnych danego przedsiębiorstwa w więcej niż jednym kraju (np. w przypadku operacji dokonywanych w międzynarodowych oddziałach danej spółki) lub też dany rodzaj przetwarzania znacznie wpływa na obywateli w więcej niż jednym kraju członkowskim (np. kiedy

administrator z innego państwa nie ma w Polsce oddziału lub spółki zależnej ale oferuje tu swoje usługi lub sprzedaje towary).

4. Świadomość dotycząca nowych przepisów w RODO

Na przygotowania do dostosowania się do nowego rozporządzenia zostało kilka miesięcy, tymczasem świadomość przedsiębiorców dotycząca RODO wciąż jest niewielka. Dotyczy to zarówno przedsiębiorców europejskich, jak i polskich. Według globalnego badania firmy Dell przeprowadzonego w 2016 roku, ponad 80% ankietowanych przedstawicieli firm nic nie wie na temat nowego unijnego rozporządzenia lub ma o nim szczątkową wiedzę. Prawie 60% respondentów z korporacji w Europie przyznało, że ich firmy nie są przygotowane na RODO lub nie znało statusu przygotowań. Podobnej odpowiedzi udzieliło niemal 70% respondentów z małych i średnich firm w tym regionie. Zaledwie 3% osób biorących udział w badaniu zadeklarowało, że ich firma ma plan wprowadzenia RODO [Michalczyk 2016]. Podobnie niepokojące są wyniki badania przeprowadzonego przez firmy IDC i ESET wśród 700 przedsiębiorstw w Czechach, Niemczech, Włoszech, Holandii, Słowacji, Hiszpanii i Wielkiej Brytanii. Pomimo dużego znaczenia zmian, które wprowadza RODO, jedna czwarta z przebadanych europejskich firm przyznała, że nie jest świadoma wymogów związanych z wdrożeniem rozporządzenia, a ponad połowa (52%) z nich nie zdaje sobie sprawy z wpływu rozporządzenia na ich organizację. Wśród tych firm, które są świadome nadchodzących zmian wprowadzanych przez rozporządzenie, co piąta firma nie zaczęła przygotowywać się do wdrożenia regulacji. Gotowych na wdrożenie jest zaledwie 21% przedsiębiorstw [*RODO już za rok...*, 2017]. Ten brak świadomości wśród przedsiębiorców jest zaskakujący, zwłaszcza w odniesieniu do potencjalnych konsekwencji, jakie mogą ponieść przedsiębiorstwa w przypadku działania niezgodnego z RODO.

Rezultaty badań dotyczących stanu implementacji wytycznych RODO w polskich organizacjach są również niepokojące. Badaniami, które w lipcu 2017 roku przeprowadziła redakcja „Computerworld" wraz z firmami Sygnity i SAS Institute, objęto 114 dyrektorów IT (CIO) reprezentujących średnie i duże przedsiębiorstwa zatrudniające co najmniej 80 pracowników. Jedynie 4% ankietowanych zadeklarowało, że już jest gotowa na wejście w życie nowych przepisów; zaś kolejne 41% przedsiębiorstw oświadczyło, że pracuje nad dostosowaniem swoich procesów i infrastruktury IT do zapisów RODO. Adaptacja ta przebiega szybciej w dużych organizacjach, z których ponad połowa (52%) zadeklarowała gotowość lub pracę nad zmianą systemów, podczas gdy w grupie organizacji średniej wielkości podobne przekonanie wyraził już niewiele więcej niż co trzeci ankietowany (Computerworld 2017). Taki wynik może wynikać z nadal istniejącego braku ostatecznych unormowań prawnych w dziedzinie ustawodawstwa krajowego, czy też jasnych wytycznych branżowych i kodeksów dobrych praktyk. W Polsce trwają już prace nad polską ustawą o danych osobowych, która uchyli obecną

i zmieni szereg przepisów. Będzie ona miała jednak przede wszystkim walor ustrojowy, określający pozycję organu, który zastąpi GIODO, sądownictwa związanego z danymi etc.

Według autorów tego badania liczne wskazania odpowiedzi „trudno powiedzieć" wskazują, że znaczna część polskich przedsiębiorców nadal nie wie, jak traktować przepisy wynikające z RODO. Podobne rezultaty uzyskali w swoim badaniu autorzy artykułu. Pilotażowe badanie zostało przeprowadzone w sierpniu 2017 roku w modelu CATI (*Computer-Assisted Telephone Interview*) oraz poprzez pojedynczy mailing CAWI (*Computer-Assisted Web Interview*) wśród przedsiębiorstw prowadzących sprzedaż internetową w województwie pomorskim. Wywiadami pogłębionymi objęto 20 firm z sektora e-commerce. Co ciekawe, wszyscy respondenci twierdzili wprawdzie o podjęciu odpowiednich działań dostosowawczych do wymogów RODO, jednak nie byli w stanie udzielić odpowiedzi na temat konkretnie podjętych kroków czy też jednoznacznie odpowiedzieć na pytanie dotyczące planów ich wdrożenia, co świadczy o nadal niskiej świadomości wymagań RODO.

Zakończenie

W skali całego sektora e-commerce pokusić się można o stwierdzenie, iż RODO jest wyjątkowo daleko idącym, trudnym i strategicznie ważnym aktem prawnym, którego prawidłowa implementacja może przynieść długofalowe korzyści zarówno dla sklepów, poprzez zwiększenie ich wiarygodności i budowę zaufania klientów, jak i dla samych klientów. Nowe zasady RODO spowodują bowiem zwiększenie świadomości konsumenta w zakresie praw do wykorzystywania jego danych osobowych. Konsument nie tylko będzie musiał zostać poinformowany o celu i sposobie przetwarzania danych osobowych, ale również będzie miał prawo do żądania od administratora danych osobowych zaprzestania ich przetwarzania oraz zapewnienia, że dane nie zostaną wydane podmiotom trzecim. Ponadto nowe regulaminy sklepów internetowych powinny również zawierać informacje o możliwości wniesienia skargi przez konsumenta do organu nadzorczego.

Tak ujęte wymagania prawdopodobnie spowodują, że administratorzy, a także podmioty przetwarzające dane na ich polecenie, będą musieli zmodyfikować metody postępowania z danymi osobowymi. Jednym z dużych wyzwań dla e-sklepów może stać się zapewnienie szybkiej procedury realizacji żądania bycia zapomnianym, jeśli potencjalna liczba zgłoszeń będzie duża. Biorąc pod uwagę fakt, że sklepy internetowe przechowują niejednokrotnie ogromne ilości danych osobowych, spełnienie dużej liczby żądań w tym samym czasie może być problemem zarówno organizacyjnym, jak i technologicznym, szczególnie jeśli w użytkowanych od lat systemach informatycznych nie ma opcji usuwania danych.

Również odpowiednie przygotowanie się do tak istotnego w e-handlu profilowania wymagać będzie przeprowadzenia przynajmniej wewnętrznego audytu

przetwarzania danych osobowych, uwzględniającego m.in. podstawę prawną profilowania danych oraz analizę środków zapewniających ochronę danych. Bardzo pomocne okaże się również z pewnością opracowanie kompleksowej polityki przetwarzania danych osobowych na potrzeby profilowania.

Wdrożenie RODO należy więc traktować jako proces a nie jednorazowe działanie, każdy zaś z e-sklepów będzie decydować o adekwatnych środkach – organizacyjnych i technicznych. Z perspektywy sklepów internetowych implementacja przepisów RODO będzie więc miała istotny wpływ zarówno na sposób zarządzania dostępem do danych, zarządzania infrastrukturą IT oraz na wykorzystanie tych danych w procesach marketingowych i sprzedażowych.

Uwagę należy również zwrócić na kolejny istotny europejski dokument, a mianowicie – rozporządzenie e-privacy, które ureguluje jednolicie w całej Unii Europejskiej zagadnienia dotyczące m.in. plików cookies, tele i e-mail marketingu oraz zasad korzystania z meta danych. W chwili obecnej rozporządzenie to jest w stadium projektu, ale planowane jest jego wejście w życie i stosowanie tych przepisów również z dniem 25 maja 2018 r.

Bibliografia

Chaffey D., 2016, *Digital business i e-commerce management. Strategia-realizacja-praktyka*, Wydawnictwo Naukowe PWN SA, Warszawa.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. U. L 281 z 23.11.1995 z późn. zm.).

Fletcher K., 2001, *Privacy: the Achilles heel of the new marketing*, "Interactive marketing", No. 3(2).

Grudzewski W.M. i in., 2009, *Zarządzanie zaufaniem w przedsiębiorstwie*, Oficyna Wydawnicza Wolters Kluwer Polska, Kraków.

Grzelak A., 2015, *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*, Wydawnictwo SGH, Warszawa.

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. Publikacja w Dz. U. z 1997 r. Nr. 78, poz. 483.

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. Publikacja w Dz. U. z 1993 r. Nr. 61, poz. 284.

Kossecki, P., 2009, *Budowanie zaufania klientów w handlu elektronicznym*, „E-Marketing.pl. Strategie marketingu internetowego", http://www.e-marketing.pl/artyk/artyk50.php (dostęp: 17.08.2017).

Maroszek W., 2016, *Ochrona danych 2.0. Nowe unijne przepisy oznaczają wiele trudności dla przedsiębiorców*, http://biznes.onet.pl/wiadomosci/ue/rodo-gdpr-regulacje-ue-o-ochronie-danych-osobowych-firma/7jmc46 (dostęp: 25.08 2017).

Michalczyk J., 2016, *Gotowość na RODO – nowe unijne rozporządzenie o ochronie danych osobowych*, „IT professional", No. 12.

Ożgalska-Trybalska J., 2001, *Adresy e-mailowe a dane osobowe*, ODO, nr 23.

Podjacki P., 2016, *Wiarygodność w e-commerce: Jakimi oznakami zaufania szczycą się europejskie sklepy internetowe?*, „E-handel", nr 2, https://ehandelmag.com/wiarygodnosc-w-e-commerce-jakimi-oznakami-zaufania-szczyca-sie-europejskie-sklepy-internetowe,1215 (dostęp: 20.08.2017).

Pryciak M., 2010, *Prawo do prywatności*, Wrocławskie Studia Erazmiańskie. Zeszyt IV. *Prawa człowieka – idea, instytucje, krytyka*, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

Przygotowania do RODO w polskich organizacjach. Świadomość wyzwania, korzyści i zagrożenia, zaawansowanie prac wdrożeniowych, oczekiwania (2017). Raport Computerworld sierpień 2017, http://www.computerworld.pl/whitepaper/2925-Przygotowania-do-RODO-w-polskich-organizacjach.html (dostęp: 8.09.2017).

RODO już za rok, a przygotowania ciągle w polu, 2017, „Egospodarka.pl", http://www.firma.egospodarka.pl/141292,RODO-juz-za-rok-a-przygotowania-ciagle-w-polu,1,11,1.html (dostęp: 8.09.2017).

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), Dz. Urz. UE z 4.05.2016, L 119/1

DATA PROTECTION IN E-COMMERCE SECTOR

SUMMARY

After four years of preparation and debate the European Union's General Data Protection Regulation (GDPR) was finally approved by the EU Parliament on 14 April 2016 and it comes into effect on 25 May 2018. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy, thus obliging also the entrepreneurs operating in Poland, including in the field of e-commerce, to adapt new regulations.

The paper analyses the challenges and implications of the changes in data protection legislation in the e-commerce industry, showing how the provisions of the regulation will affect this sector. The paper focuses on main changes in data protection, including the modification of the consent form for data processing, increased control over personal data, information on data protection breaches and the conditions for admissibility of data transfer to a third country. For this purpose, the following research methods were used: literature study, intuitive method and descriptive statistics method. Pilot studies have also been conducted among entrepreneurs providing e-commerce services in Poland using the in-depth interview method and questionnaire surveys.

Keywords: data protection, electronic commerce.