PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU
RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS nr 487 • 2017

Polityka ekonomiczna

ISSN 1899-3192
e-ISSN 2392-0041

Andrzej Kamiński, Krystian Dąbek
Uniwersytet Ekonomiczny we Wrocławiu
e-mails: andrzej.kaminski@advisor-kbu.pl, dkrystian@interia.eu

NOWE ZAGROŻENIA DLA DZIAŁALNOŚCI PRZEDSIĘBIORSTW W ŚWIETLE ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO O OCHRONIE DANYCH OSOBOWYCH (RODO)

NEW THREATS FOR THE OPERATION OF ENTERPRISES IN THE LIGHT OF THE EUROPEAN PARLIAMENT'S GENERAL DATA PROTECTION REGULATION (GDPR)

DOI: 10.15611/pn.2017.487.12
JEL Classification: K20, K23

Streszczenie: Omawiane w artykule Rozporządzenie Parlamentu Europejskiego o ochronie danych osobowych (zwane w skrócie RODO) wejdzie w życie w maju 2018 r. i będzie obowiązywało we wszystkich krajach członkowskich. Celem wprowadzonej regulacji jest unifikacja prawa unijnego w zakresie bezpieczeństwa danych osobowych wobec wzrastającej z roku na rok liczby incydentów naruszenia bezpieczeństwa danych. Celem opracowania jest zidentyfikowanie zagrożeń dla przedsiębiorstw wynikających z wdrożenia Rozporządzenia Parlamentu Europejskiego o ochronie danych osobowych. Artykuł składa się z czterech części. W pierwszej przedstawiono wyniki krajowych i zagranicznych badań nad ekspozycją przedsiębiorstw na ryzyko zmian prawnych, natomiast w drugiej sprecyzowano istotę zagrożeń wynikających z wprowadzenia RODO. W trzeciej części scharakteryzowano wybrane obowiązki nałożone na przedsiębiorstwa w kontekście ich oddziaływania na sytuację ekonomiczną podmiotu. W czwartej zaś przybliżono finansowe skutki nieprzestrzegania przepisów rozporządzenia.

Słowa kluczowe: dane osobowe, dane wrażliwe, ryzyko zmian prawnych, zarządzanie ryzykiem.

Summary: The following article discusses the European Parliament's General Data Protection Regulation (GDPR), which will become effective in May 2018 in all EU member states. The aim of the newly introduced regulation is to unify the EU law in terms of personal data security in the face of the increasing number of incidents relating to data security breach.The aim of the study is to identify threats to companies resulting from the implementation of the General Data Protection Directive of the European Parliament. The article consists of four parts. The first part presents the results of domestic and foreign research on exposure of enterprises to

the risk of legal changes, while the second part specifies the nature of corporate risk related to the introduction of GDPR. In the third part, selected responsibilities of companies are characterized in the context of the impact on their economic situation. Finally, the fourth part focuses on the financial consequences of failure to comply with the provisions of the regulation.

Keywords: personal data, sensitive data, risk of legal changes, risk management.

1. Wstęp

Każda aktywność człowieka zarówno w sferze życia osobistego, zawodowego, jak i gospodarczego wiąże się z ryzykiem. Każde przedsiębiorstwo bez względu na formę organizacyjną, strukturę własności czy wielkość, prowadząc swoją działalność, musi brać pod uwagę ryzyka naturalne, techniczne, gospodarcze, finansowe, prawne, polityczne czy społeczne.

Sieć coraz silniejszych zależności wynikających z globalizacji kreuje nowe zagrożenia dla przedsiębiorstw. Dynamicznie wzrastają np. niepewność pochodząca z otoczenia prawnego, groźba utraty reputacji czy zagrożenie cyber-przestępczością. Na szczególną uwagę zasługuje ryzyko zmian prawnych. Niniejszy artykuł stanowi próbę spojrzenia na wprowadzenie nowych, obowiązujących w całej Unii Europejskiej regulacji w zakresie ochrony danych osobowych z perspektywy zagrożeń, jakie ze sobą niosą, dla podmiotów gospodarczych, instytucji i urzędów (zwanych dalej dla uproszczenia rozważań „przedsiębiorstwami" lub „administratorami").

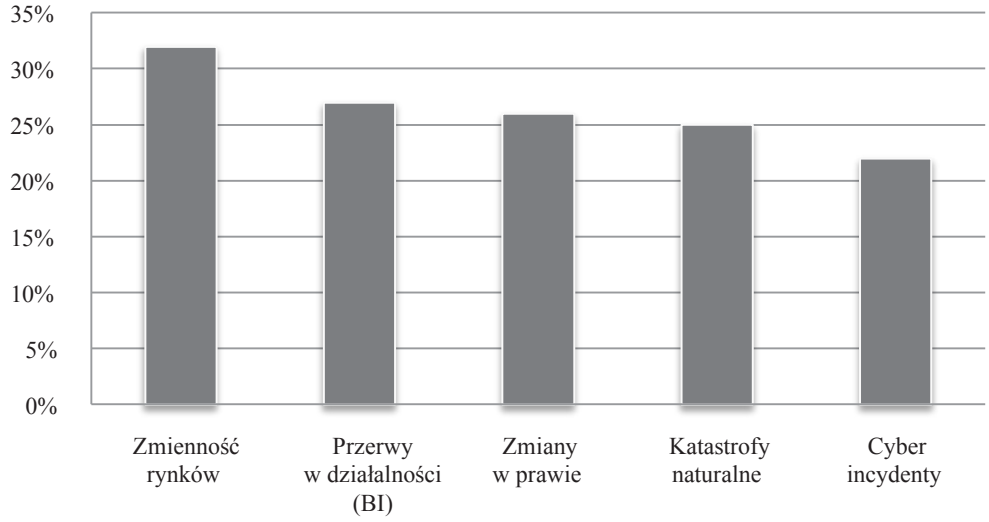
Celem opracowania jest zidentyfikowanie zagrożeń dla przedsiębiorstw wynikających z wdrożenia Rozporządzenia Parlamentu Europejskiego o ochronie danych osobowych (RODO). Opracowanie zostało podzielone na cztery części. W pierwszej przedstawiono wyniki krajowych i zagranicznych badań nad ekspozycją przedsiębiorstw na ryzyko zmian prawnych, natomiast w drugiej sprecyzowano, na czym polega ryzyko przedsiębiorstw związane z wprowadzeniem RODO. W trzeciej części scharakteryzowano wybrane obowiązki w kontekście ich oddziaływania na sytuację ekonomiczną przedsiębiorstwa, w czwartej zaś przybliżono finansowe skutki nieprzestrzegania przepisów rozporządzenia.

2. Ryzyko zmian prawnych jako jedno z głównych zagrożeń dla przedsiębiorstw

Prowadzone cyklicznie przez Światowe Forum Ekonomiczne badania nad ekspozycją gospodarki światowej na poszczególne ryzyka wskazują, że w miarę rozwoju technologicznego, postępującej cyfryzacji i wirtualizacji systemów zarządzania następuje wzrost znaczenia niematerialnych źródeł potencjalnych strat finansowych w porównaniu z typowymi szkodami materialnymi, takimi jak np. katastrofy natu-

ralne czy zniszczenie składników majątkowych [World Economic Forum… 2017, s. 3].

Inne badania międzynarodowych organizacji potwierdzają wzrost świadomości nowych ryzyk wśród zarządzających.



Rys. 1. Źródła największych zagrożeń dla działalności firm z sektora małych i średnich przedsiębiorstw (MŚP) w 2015 r.

Źródło: opracowanie własne na podstawie [Allianz Risk Barometer … 2017].

Raport Allianz Risk Barometer: *Business Risks 2017* wskazuje najważniejsze ryzyka towarzyszące działalności gospodarczej [Allianz Risk Barometer… 2017, s. 13]. Niestabilność rynków, przerwy w działalności spowodowane czynnikami wewnętrznymi i zewnętrznymi, zbyt częste i zaskakujące zmiany prawne, katastrofy naturalne oraz incydenty cybernetyczne wzbudzają największe obawy o ciągłość działalności. W zestawieniu pięciu najczęściej wskazywanych – przez ponad 500 menedżerów z małych i średnich firm z 40 krajów świata – największych zagrożeń dla działalności, pokazanym na rys. 1, mamy tylko jedno *stricte* materialne ryzyko katastrof naturalnych. Drugie ryzyko – przerw w działalności – jest nim tylko częściowo, bo zakłócenie ciągłości działalności lub przerwanie łańcucha dostaw może być spowodowane zarówno pożarem czy powodzią, jak i awarią systemów informatycznych w wyniku ataku hakerskiego. Pozostałe ryzyka: zmienność rynków, zmienność regulacji prawnych i incydenty cybernetyczne, mają charakter niematerialny.

W Polsce zjawisko coraz większej ekspozycji na ryzyka niematerialne jest również zauważalne (tab. 1). Jak wynika z raportu *Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce*, na 53 rozpatrywane czynniki ryzyka w działalności

gospodarczej respondenci uplasowali w pierwszej dziesiątce jedynie 3 materialne, tj. przerwy w działalności na 6. miejscu oraz straty w mieniu i awarie systemów informatycznych na 9. i 10. pozycji [*Zarządzanie ryzykiem*… 2017, s. 7].

Tabela 1. Ranking ryzyk pod względem zagrożenia dla działalności gospodarczej w Polsce

Rodzaj ryzyka	Pozycja w rankingu Polska	Pozycja w rankingu światowym
Wzrost konkurencji	1	4
Spowolnienie gospodarcze	2	2
Zmiany regulacji prawnych	**3**	**3**
Utrata reputacji	4	1
Ceny towarów	5	11
Przerwa w prowadzeniu działalności	6	7
Należności handlowe/płatności kontrahentów	7	27
Zmienność kursów walutowych	8	17
Zniszczenie, uszkodzenie mienia	9	10
Awaria systemów informatycznych	10	13

Źródło: opracowanie własne na podstawie [*Zarządzanie ryzykiem*… 2017].

Wnioski z badań światowych i polskich pokrywają się w znacznym stopniu. Ani w polskim badaniu, ani w światowym w pierwszej piątce nie znalazły się materialne źródła strat. Widocznym znakiem zachodzących zmian w podejściu do niematerialnych źródeł potencjalnych szkód jest rosnące zagrożenie związane ze zmianami prawnymi. We wszystkich przytaczanych badaniach ryzyko zmian w ustawodawstwie i przepisach prawnych jest uznawane za jedno z trzech najważniejszych zagrożeń dla działalności przedsiębiorstwa.

3. Znaczenie unijnych przepisów o ochronie danych osobowych dla przedsiębiorstw

Problemy z zachowaniem bezpieczeństwa danych w sytuacji dynamicznego rozwoju cyfrowych metod ich przetwarzania zostały dostrzeżone przez Unię Europejską. Podjęto prace nad ujednoliceniem i uaktualnieniem prawnych aspektów związanych z ochroną danych, ze szczególnym uwzględnieniem danych osobowych. W konsekwencji przyjęto 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 (w dalszej części artykułu zwane w skrócie „Rozporządzeniem" lub „RODO").

Uchwalone przepisy Rozporządzenia wejdą w życie po dwuletnim okresie przygotowawczym. Z dniem 25 maja 2018 r. zastąpią dotychczasową dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. Na podstawie

art. 288 Traktatu o funkcjonowaniu Unii Europejskiej Rozporządzenie będzie obowiązywało na całym jej obszarze. Wszystkie państwa wspólnoty będą zobligowane do stosowania jego przepisów wprost, bez konieczności implementacji do krajowych przepisów o ochronie danych osobowych [Karwala 2016]. W rezultacie obowiązujące w Polsce przepisy utracą swą moc w zasadniczej części[1], a inne przepisy branżowe będą wymagać dostosowania do unijnej regulacji.

Rozporządzenie rozciąga obowiązek stosowania nowych regulacji niemal na wszystkich gestorów baz danych osobowych. Rozporządzenie bowiem za „przetwarzanie" uznaje każdą operację wykonywaną na danych osobowych, taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Nie ma tu znaczenia, czy operacje na danych wykonywane są w sposób zautomatyzowany lub niezautomatyzowany [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 4 pkt 2].

Administratorem danych będzie każda osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Zatem każdy podmiot prowadzący rejestr, np. klientów czy pracowników, będzie administratorem danych [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 4 pkt 7 i 8].

W praktyce oznacza to, że każdy podmiot będzie podlegał przepisom Rozporządzenia, nawet taki, który prowadzi jednoosobowo działalność gospodarczą. Osoba prowadząca działalność gospodarczą na własny rachunek lub w ramach samozatrudnienia również będzie podlegać przepisom Rozporządzenia albo jako administrator danych, gdy prowadzi własne rejestry, albo jako „podmiot przetwarzający", gdy dokonuje przetwarzania danych w rejestrach innego podmiotu będącego administratorem, np. w związku z umową łączącą te podmioty. Rozporządzenie bowiem za podmiot przetwarzający uważa każdą osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Rozporządzenie wprowadza wiele znaczących zmian, jednakże w dalszej części artykułu zostaną przedstawione wybrane obowiązki formalne, nowe sankcje administracyjne i finansowe oraz zaostrzone zasady odpowiedzialności cywilnej, które z perspektywy podmiotów przetwarzających dane osobowe mogą być postrzegane jako źródło zagrożeń w ich działalności.

[1] Według stanu na czerwiec 2017 r. nowy projekt ustawy o ochronie danych osobowych złożony przez Ministerstwo Cyfryzacji jest przedmiotem prac legislacyjnych.

4. Zwiększone koszty działalności związane z obowiązkiem prowadzenia rejestru czynności przetwarzania, dokonywania oceny skutków przetwarzania oraz zgłaszania naruszenia ochrony danych

Rozporządzenie nakłada na administratorów obowiązek rejestrowania czynności przetwarzania danych osobowych [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 30]. Z uwagi na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw Rozporządzenie przewiduje wyjątek dla podmiotów zatrudniających mniej niż 250 pracowników. Pozostałe przedsiębiorstwa muszą liczyć się z koniecznością ponoszenia zwiększonych kosztów operacyjnych.

Rozporządzenie określa ponadto, że jeżeli dany rodzaj przetwarzania, zwłaszcza z użyciem nowych technologii – ze względu na swój charakter, zakres i cele – wiąże się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 35 ust. 1]. Oceny skutków należy zawsze dokonywać, gdy stosuje się profilowanie, przetwarza się dane wrażliwe na dużą skalę, monitoruje się na dużą skalę miejsca publiczne, przetwarza się dane określone przez nadzór. Dokonanie oceny skutków wymaga wiedzy eksperckiej i polega na opisie planowanych operacji przetwarzania i ich celów, ocenie adekwatności przetwarzania w stosunku do celów, ocenie zagrożenia dla praw i wolności osób, ocenie środków prewencyjnych i ochronnych. Dlatego administratorzy będą zobowiązani powołać Inspektora Ochrony Danych (IOD), co stanowi kolejne obciążenie finansowe.

Rozporządzenie nakłada na wszystkich administratorów również obowiązek zgłaszania incydentów naruszenia ochrony danych osobowych. Przez „naruszenie ochrony danych osobowych" rozumieć należy naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

W sytuacji, w której taki incydent mógłby naruszać prawa lub wolności osób fizycznych, administrator zgłasza fakt do organu nadzorczego, którego rolę w Polsce pełni Generalny Inspektor Ochrony Danych Osobowych (GIODO). Natomiast podmiot przetwarzający, po stwierdzeniu naruszenia ochrony danych osobowych, jest zobowiązany niezwłocznie raportować do administratora [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 33 ust. 1 i 2].

Dodatkowo Rozporządzenie wprowadza nowy obowiązek prowadzenia przez administratora danych osobowych dokumentacji w zakresie wszelkich naruszeń ochrony danych osobowych. Oznacza to, że nawet w sytuacji, w której administra-

tor nie ma obowiązku poinformowania GIODO o naruszeniu, musi i tak odnotować je w swojej dokumentacji. Jest to kolejny, obok wspomnianego wyżej rejestru czynności przetwarzania, rejestr obowiązkowy dla wszystkich administratorów. Ustawiczne prowadzenie takiej dokumentacji zgodnie z wymogami nowych regulacji wymagać będzie dodatkowych nakładów finansowych.

Należy podkreślić, że każdorazowe, obowiązkowe zgłoszenie naruszenia danych wiąże się niejako automatycznie z ryzykiem sankcji administracyjnych, w tym kar finansowych, do których nakładania Rozporządzenie uprawnia organ nadzorczy. Oznacza również zagrożenie utratą reputacji, bo należy się spodziewać, że organ nadzoru będzie podawał do publicznej wiadomości informacje o sankcjach w celu spełnienia ich funkcji odstraszającej. Ponadto w sytuacji, w której przedmiotowe naruszenie niesie wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator powinien również bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o takim naruszeniu – jasnym i prostym językiem [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 34 ust. 1 i 2]. Obowiązek poinformowania o naruszeniu bezpieczeństwa wszystkich poszkodowanych klientów, szczególnie dla podmiotów masowo przetwarzających dane, może być bardzo kosztowne, zarówno operacyjnie, jak i wizerunkowo. Należy podjąć działania w celu zmniejszenia ryzyka np. wycieków danych. Przedsiębiorstwa będą musiały uwzględnić większy budżet na wdrożenie mechanizmów zabezpieczenia danych osobowych oraz zabezpieczyć finansowanie ewentualnych kampanii mailingowych.

5. Rozszerzone sankcje finansowe oraz zaostrzona odpowiedzialność cywilna za przetwarzanie danych niezgodne z Rozporządzeniem

Przepisy obowiązujące przed wprowadzeniem Rozporządzenia przewidują stosunkowo niskie sankcje za nieprzestrzeganie ustawy o ochronie danych osobowych [Ustawa z 29 sierpnia 1997 r., art. 49]. Przykładowo za niedopuszczalne przetwarzanie danych albo przetwarzanie bez uprawnień grozi grzywna, kara ograniczenia wolności albo pozbawienia wolności do 2 lat. W przypadku danych wrażliwych kara pozbawienia wolności jest podwyższona do 3 lat. Aby doszło do ich zastosowania, podmiot musiał uporczywie uchylać się od nakazu zaprzestania nielegalnych praktyk. Nawet wtedy grzywny nie były dotkliwe, a sankcje karne rzadko stosowane.

Rozporządzenie nadaje krajowemu organowi nadzorczemu szereg uprawnień naprawczych oraz wprowadza nowe sankcje za niezgodne z prawem przetwarzanie danych osobowych. Organ nadzoru ma prawo decyzji, czy skorzysta z upomnienia, ostrzeżenia czy innego nakazu administratora, czy też zamiast lub oprócz nich nałoży administracyjną karę pieniężną [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 58 ust. 2; art. 83 ust. 2].

Rozporządzenie wymaga, aby stosowane administracyjne kary pieniężne były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające. Rozporządzenie dopuszcza na mocy art. 84 wprowadzenie przez państwa członkowskie dodatkowych sankcji, w tym karnych. Za naruszenie istotnych przepisów ochrony danych osobowych Rozporządzenie przewiduje grzywnę maksymalnie do 20 mln EUR, a w przypadku przedsiębiorstwa do 4% całkowitego światowego obrotu z poprzedniego roku. Rozporządzenie przewiduje o połowę mniejsze kary finansowe (10 mln EUR lub do 2% światowego obrotu) za uchybienia mniejszego znaczenia, jak np. naruszenie przez administratora obowiązku dokonania oceny skutków przetwarzania danych lub obowiązku powołania IOD. Każdy przypadek działania niezgodnego z przepisami Rozporządzenia GIODO będzie musiał rozpatrzyć indywidualnie, biorąc pod uwagę m.in.: skalę naruszenia, umyślność działania, działania podjęte w celu zminimalizowania szkody, historię ewentualnych poprzednich zgłoszeń, stopień współpracy z GIODO oraz rodzaj danych osobowych. Należy się spodziewać surowszego podejścia nadzoru do naruszeń danych wrażliwych. W praktyce oznacza to, że nieuchronność sankcji i zagrożenie bardzo wysokimi grzywnami zmusi administratorów do przykładania większej wagi do respektowania przepisów Rozporządzenia, a w konsekwencji do przeznaczania większych środków w swoich budżetach na ochronę informacji i bezpieczeństwo danych.

W art. 82 Rozporządzenie literalnie wskazuje podstawę i adresata potencjalnych roszczeń. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów Rozporządzenia, ma prawo do uzyskania od administratora lub podmiotu przetwarzającego odszkodowania za poniesioną szkodę [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 82 ust. 1]. O ile sama zasada obligująca sprawcę szkody do jej naprawienia jest obecna w polskim prawie cywilnym w postaci art. 415 i 448 kc [Bieniek (red.) 2001], to dalsze ustępy art. 82 Rozporządzenia zaostrzają zasady odpowiedzialności cywilnej za szkody spowodowane przetwarzaniem danych niezgodnym z Rozporządzeniem.

Odpowiedzialnością za przetwarzanie danych niezgodnie z Rozporządzeniem obciążony jest każdy administrator, ale również podmiot przetwarzający działający na polecenie administratora, o ile nie dopełnił obowiązków określonych Rozporządzeniem lub działał niezgodnie z instrukcjami administratora lub wbrew tym instrukcjom [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 82, ust. 2].

Administrator i podmiot przetwarzający mogą zostać zwolnieni z odpowiedzialności tylko wtedy, gdy udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Tym samym Rozporządzenie odchodzi od upowszechnionej w prawie cywilnym zasady, iż ciężar dowodu spoczywa na osobie występującej z roszczeniem [Dmowski, Rudnicki 2001]. Klient kierujący do administratora lub podmiotu przetwarzającego roszczenie o naprawienie szkody lub zadośćuczynienie za naruszenie dóbr osobistych w związku z niezgodnym z prawem przetwarzaniem jego danych osobowych nie będzie musiał, jak

dotychczas, dowieść swojej szkody oraz wykazać, w jaki sposób strona pozwana przyczyniła się do jej powstania. W nowej rzeczywistości prawnej to pozwany administrator lub podmiot przetwarzający będzie musiał dowieść, że nie ponosi winy za zdarzenie, np. że z całą pewnością w ciągu całego okresu przetwarzania, na żadnym w jego etapów nie doszło do naruszenia danych osobowych. Biorąc pod uwagę realia pracy wielu podmiotów gospodarczych, instytucji czy urzędów (braki organizacyjne i kadrowe, niedoinwestowanie, przestarzała infrastruktura informatyczna), można przypuszczać, że uwolnienie się od odpowiedzialności poprzez wykazanie braku winy za zdarzenie będzie w praktyce często niemożliwe.

W celu zagwarantowania osobie poszkodowanej realnego zaspokojenia jej roszczeń Rozporządzenie wprowadza odpowiedzialność solidarną. W sytuacji, kiedy w przetwarzaniu uczestniczy więcej podmiotów (administratorów lub podmiotów przetwarzających), np. kiedy dany pacjent w trakcie leczenia został skierowany przez lekarza do przychodni, a ta dalej skierowała go do szpitala lub innych placówek, to pacjent ma prawo dowolnie wybrać, do którego podmiotu będzie składał roszczenie, np. o ujawnienie wyników badań diagnostycznych. Może również skierować roszczenia oddzielnie do wszystkich lecznic. Wszystkie podmioty lecznicze, które nie będą mogły dowieść, że wina nie leży po ich stronie, zostaną obarczone odpowiedzialnością cywilną i będą zobowiązane wspólnie ponieść koszty odszkodowania. Jeśli jeden z odpowiedzialnych podmiotów okazałby się niewypłacalny (np. ze względu na upadłość), inni odpowiedzialni byliby zmuszeni pokryć brakującą część odszkodowania.

Jeśli jeden podmiot został uznany za winnego i wypłacił odszkodowanie pokrywające całość szkody, to ma prawo dochodzenia od innych podmiotów, które uczestniczyły w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność (prawo do regresowania) [Rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r., art. 82 ust. 5]. Zatem podmioty, które uczestniczyły w tym samym przetwarzaniu, których poszkodowany nie wybrał pierwotnie jako adresatów swojego roszczenia, nie będą mogły uznać sprawy za zamkniętą. Roszczenia regresowe mogą bowiem pojawić się z opóźnieniem.

Przeniesienie ciężaru dowodu, wprowadzenie odpowiedzialności solidarnej, swobodny wybór poszkodowanego co do adresatów roszczeń oraz możliwość ich późniejszego regresowania znacząco ułatwią potencjalnym poszkodowanym dochodzenie swoich praw, co jest celem prokonsumenckich rozwiązań wdrażanych w UE. Jednakże dla drugiej strony ewentualnego sporu, czyli dla każdego przedsiębiorstwa uznanego za administratora lub podmiot przetwarzający, ryzyko prawne znacząco wzrasta. Wyraźne zaostrzenie zasad odpowiedzialności może być potencjalnym źródłem fali odszkodowań (w tym wielu nienależnych, lecz uznanych wobec niemożności dowiedzenia „niewinności"). W celu przeciwdziałania negatywnym skutkom roszczeń administratorzy będą zmuszeni monitorować przetwarzanie danych na każdym etapie i dokumentować czynności przetwarzania, tak aby

w razie ewentualnego sporu móc wykazać brak swojej winy. Przedsiębiorstwa będą zmuszone ponieść ogromny wysiłek organizacyjny i finansowy na stworzenie odpowiednich procedur, szkolenia i niezbędną infrastrukturę techniczną i informatyczną. Rozporządzenie nakazuje wprost prowadzenie działań tego rodzaju, wprowadzając nową, nieznaną dotychczas zarówno prawu unijnemu, jak i krajowemu tzw. zasadę rozliczalności (*accountability*). Zasada wymaga opracowania i wdrożenia polityki bezpieczeństwa informacji, wielu procedur wewnętrznych, w tym awaryjnych planów zarządzania ciągłością, prowadzenia rozbudowanej dokumentacji, szkoleń dla pracowników wszystkich szczebli, zewnętrznych audytów zgodności itp., co ma dać szansę obrony przed sankcjami administracyjnymi, karami finansowymi oraz przed roszczeniami z tytułu odpowiedzialności cywilnej.

6. Zakończenie

Rozporządzenie o ochronie danych osobowych (RODO) jest oczekiwanym spójnym, prokonsumenckim narzędziem przeciwdziałającym rosnącej fali naruszeń danych osobowych. Niemal wszystkie przedsiębiorstwa jako administratorzy będą zmuszone stosować się do tych samych zasad ochrony danych osobowych, tj. zasady zgodności z prawem, rzetelności i przejrzystości, zasady ograniczenia celu, zasady minimalizacji danych, ograniczenia przechowywania oraz prawidłowości, integralności i poufności. Zgodnie z nową zasadą rozliczalności dodatkowo będą zobligowane tak prowadzić wewnętrzną politykę bezpieczeństwa informacji, aby móc dowieść przestrzegania tych zasad. Zaostrzone wymagania formalne i zasady odpowiedzialności będą konsekwentnie egzekwowane pod sankcją wysokich kar finansowych. Nowe przepisy ułatwiają osobom poszkodowanym, a nawet zachęcają, dochodzenie odszkodowań na drodze cywilnej.

Powyższe zmiany prawne będą miały znaczny wpływ nie tylko na sytuację prawną, ale i ekonomiczną niemal wszystkich przedsiębiorstw, które na co dzień przetwarzają dane osobowe swoich klientów czy pracowników. Poszerzone obowiązki i zwiększone wymagania będą wyzwaniem organizacyjnym, technicznym, a w konsekwencji finansowym. Natomiast zwiększone prerogatywy nadzoru i szerszy niż dotychczas katalog sankcji mogą budzić obawy o ciągłość działalności przedsiębiorstwa.

W celu spełnienia obowiązków nałożonych przepisami Rozporządzenia przedsiębiorstwa będą zmuszone przeorganizować swoje strategie bezpieczeństwa poprzez ściślejsze połączenie technologii, procesów i kwalifikacji pracowników. W praktyce przekłada się to na dodatkowe działania operacyjne związane z bardziej zaawansowanymi procedurami i wewnętrzną kontrolą przetwarzania danych, zwiększone nakłady na infrastrukturę techniczną i systemy bezpieczeństwa danych oraz na szkolenia pracowników wszystkich szczebli, a także na usługi eksperckie. W rezultacie przedsiębiorstwa (w szczególności małe i średnie) muszą liczyć się

ze zwiększeniem kosztów operacyjnych, co może być znaczącym zagrożeniem dla ich sytuacji ekonomicznej.

Nawet przy nieograniczonym budżecie i zastosowaniu wszelkich możliwych procedur i zabezpieczeń, w sytuacji nieustannego rozwoju cyberprzestępczości, ryzyko naruszenia danych nie zostanie jednak wyeliminowane. Przedsiębiorstwa stają przed widmem nieuchronnych sankcji i dotkliwych kar finansowych. Pojawiają się dodatkowe koszty skutecznego powiadomienia wszystkich poszkodowanych, koszty specjalistycznych usług (np. informatyka śledcza) i nakłady na PR w celu przeciwdziałania utracie reputacji. Wzmocnienie pozycji poszkodowanego w sporze cywilnym sprawi, że taki incydent w niedługim czasie może odbić się echem w postaci indywidualnych roszczeń lub pozwów zbiorowych z tytułu odpowiedzialności cywilnej. Każde przedsiębiorstwo powinno zawczasu oszacować koszty obsługi sporów oraz prawdopodobieństwo i wysokość ewentualnych odszkodowań, a następnie uwzględnić je w planach finansowych.

Tak szeroki zakres zmian prawnych związanych z wejściem w życie Rozporządzenia wymaga podjęcia przedsięwzięć organizacyjnych, inwestycji technicznych oraz odpowiedniego zabezpieczenia finansowego dla zapewnienia zgodności z nowymi przepisami. Należy zatem wnioskować, iż wprowadzenie w życie Rozporządzenia generować będzie w przedsiębiorstwie stałe koszty operacyjne zależne od branży i jego wielkości oraz koszty nadzwyczajne zależne od ryzyka wystąpienia uchybień wobec przepisów Rozporządzenia.

Powyższe czynniki stanowią niewątpliwe zagrożenia dla ciągłości działania, a nawet bytu przedsiębiorstwa, dlatego powinny być uwzględnione w strategii zarządzania ryzykiem w każdym przedsiębiorstwie.

Literatura

Allianz Risk Barometer: *Business Risks 2017*, 2017, Allianz Global Corporate & Specialty, https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf (5.06.2017).

Bieniek G. (red.), 2001, *Komentarz do Kodeksu Cywilnego, Księga trzecia, Zobowiązania*, Wydawnictwo Prawnicze, Warszawa.

Dmowski S., Rudnicki S., 2001, *Komentarz do Kodeksu Cywilnego, Księga pierwsza, Część ogólna*, Wydawnictwo Prawnicze, Warszawa.

Karwala D., 2016, *Wpływ ogólnego rozporządzenia o ochronie danych osobowych na działalność zakładów ubezpieczeń – zagadnienia wybrane*, Prawo Asekuracyjne, nr 4(89), Fundacja „Prawo Ubezpieczeniowe", Warszawa, s. 17–31.

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), http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL (30.03.2017).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t.j. Dz.U. 2016, poz. 922.

World Economic Forum *The Global Risks Report 2017*, 2017, http://www3.weforum.org/docs/GRR17_Report_web.pdf (5.06.2017).

Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce – IV edycja PL, (2017), Aon Polska, http://www.aon.com/poland/risk/Aon%20Thought%20Leadership/Zarzadzanie-ryzykiem-i-ubezpieczeniami-w-Polsce-IV-edycja.jsp (18.06.2017).