Damian Karwala

Wpływ ogólnego rozporządzenia o ochronie danych osobowych na działalność zakładów ubezpieczeń – zagadnienia wybrane

Przyjęcie rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r. o ochronie danych zakończyło trwające ponad 4 lata prace nad reformą unijnych ram prawnych w zakresie ochrony danych osobowych. Przepisy rozporządzenia mają zastąpić dyrektywę 95/46/WE oraz, w zasadniczej części, ustawę o ochronie danych osobowych; wpłyną one również na interpretację regulacji sektorowej – ustawy o działalności ubezpieczeniowej i reasekuracyjnej. Szczególne znaczenie z perspektywy zakładów ubezpieczeń mają rozwiązania, które dotyczą takich instytucji, jak: podstawa przetwarzania danych w postaci zgody podmiotu danych; profilowanie, w szczególności prowadzące do zautomatyzowanego podejmowania decyzji; przekazywanie danych osobowych w ramach grup kapitałowych, w tym do państw trzecich; wreszcie – z uwagi na wprowadzenie możliwości nakładania przez organy nadzorcze kar pieniężnych – podstawowe zasady odpowiedzialności z tytułu naruszenia przepisów rozporządzenia.

Słowa kluczowe: rozporządzenie o ochronie danych osobowych, zgoda podmiotu danych, profilowanie, odpowiedzialność administracyjna (finansowa) administratora danych.

1. Uwagi wprowadzające

W dniu 27 kwietnia 2016 r. Parlament Europejski przyjął ogólne rozporządzenie o ochronie danych osobowych[1], kończąc w ten sposób trwające ponad 4 lata prace w tym zakresie. Akt ten, po 2-letnim okresie dostosowawczym, w pierwszej połowie 2018 r. (z dniem 25 maja 2018 r.), ma zastąpić dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2], jak również – w zasadniczej części – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[3]. Rozporządzenie unijne, z uwagi na zasadę bezpośredniego obowiązywania i stosowania jego przepisów (art. 288 Traktatu o funkcjonowaniu Unii Europejskiej), nie wymaga przyjmowania krajowych przepisów, które dokonywałyby implementacji ogólnego rozporządzenia. Dostosowania do nowych przepisów

[1] 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 L 119, z 4.05.2016 r., s. 1; dalej: „ogólne rozporządzenie" lub „rozporządzenie").

[2] Dz. U. UE L 281, z 23.11.1995 r., s. 31, dalej: „dyrektywa 95/46/WE" lub „dyrektywa".

[3] Tekst jedn. Dz. U. z 2016 r. poz. 922, z późn. zm.

wymagać może jednak regulacja sektorowa, w tym ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej[4], która dotyczy również w określonym zakresie problematyki ochrony danych osobowych (np. art. 41 ust. 2). W każdym jednak przypadku – bez względu na podjęcie przez krajowego ustawodawcę odpowiednich kroków – niezbędne będzie stosowanie takiej interpretacji przepisów krajowych, która pozwoli na zapewnienie ich zgodności z ogólnym rozporządzeniem.

2. Najważniejsze zmiany

Wśród najważniejszych zmian, jakie w zakresie regulującym problematykę związaną z ochroną danych osobowych wprowadza ogólne rozporządzenie, wskazać należy następujące zagadnienia:

- zmiana dotycząca terytorialnego zakresu zastosowania unijnych przepisów w stosunku do podmiotów (administratorów oraz – co ciekawe – również podmiotów przetwarzających dane) spoza UE, w szczególności zastąpienie przesłanki korzystania ze środków (technicznych) znajdujących się na terytorium UE (Polski) przesłanką oferowania towarów lub usług odbiorcom w UE lub monitorowania ich zachowania, o ile do zachowania tego dochodzi w Unii (art. 3 ust. 2);
- doprecyzowanie wymogów w zakresie zgody, jako podstawy przetwarzania danych osobowych (zob. dalsze, szczegółowe uwagi w tym zakresie);
- wzmocnienie podstawowych zasad przetwarzania danych, w szczególności przez podkreślenie znaczenia takich zasad, jak zasada przejrzystości (transparentności), zasada minimalizacji zakresu oraz ilości przetwarzanych danych oraz zasada integralności i poufności (art. 5 ust. 1);
- wprowadzenie nieznanej dotychczas unijnej oraz krajowej regulacji zasady rozliczalności (ang. *accountability*), która wymaga m.in. inwestycji w wewnętrzną organizację ochrony danych w przedsiębiorstwie administratora (procesora) danych, w tym m.in. prowadzenia rozbudowanej dokumentacji wewnętrznej (m.in. rejestru czynności przetwarzania – art. 30, jak również różnego rodzaju polityk i procedur wewnętrznych); wyznaczenia – w określonych sytuacjach – inspektora ochrony danych (odpowiednika administratora bezpieczeństwa informacji); prowadzenia wewnętrznych szkoleń, w tym na najwyższym poziomie kadry menedżerskiej; oceny skutków itd. (art. 5 ust. 2);
- wprowadzenie nowych lub istotnie zmodyfikowanych uprawnień podmiotów, których dane dotyczą, takich jak „prawo do bycia zapomnianym" (ang. *right to be forgotten*, art. 17), „prawo do ograniczenia przetwarzania" (art. 18), czy też „prawo do przenoszenia danych" (ang. *right to data portability*, art. 20);
- uregulowanie profilowania, w szczególności prowadzącego do podejmowania decyzji w sposób zautomatyzowany, jako szczególnego rodzaju operacji na danych osobowych (zob. dalsze uwagi);

[4] Dz. U. z 2015 r. poz. 1844.

– nałożenie wymogu stosowania zasad ochrony danych *„by design"* (wymagającego uwzględnienia ochrony prywatności już na etapie projektowania określonych rozwiązań, produktów lub usług; art. 25 ust. 1) oraz ochrony danych *„by default"* (wymagającego przyjmowania określonych ustawień chroniących prywatność jako domyślnych; art. 25 ust. 2);
– wprowadzenie obowiązku przeprowadzania oceny skutków dla ochrony danych (tzw. ocena wpływu na prywatność; ang. *privacy impact assessment*; art. 35) oraz prowadzenia uprzednich konsultacji z organem nadzorczym (art. 36);
– zniesienie obowiązku notyfikacji organom nadzorczym operacji przetwarzania danych osobowych (na gruncie krajowej ustawy – rejestracji zbiorów danych);
– wprowadzenie powszechnego obowiązku zgłaszania naruszeń ochrony danych (ang. *data breach notification*), zarówno organowi nadzorczemu (art. 33), jak również podmiotom, których dane dotyczą (art. 34);
– doprecyzowanie sytuacji prawnej podmiotów przetwarzających dane (tzw. procesorów danych; art. 28 i in. rozporządzenia);
– wprowadzenie obowiązku wyznaczenia inspektora ochrony danych (ang. *data protection officer*) m.in. przez podmioty, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, w tym danych o stanie zdrowia (co znajdzie zastosowanie w stosunku do zakładów ubezpieczeń, w szczególności tych oferujących ubezpieczenia na życie);
– wdrożenie określonych usprawnień w kontekście operacji przekazywania danych osobowych do państw trzecich, m.in. poprzez wyraźne uznanie wiążących reguł korporacyjnych oraz wprowadzenie nowych instrumentów transferowych w postaci kodeksów dobrych praktyk oraz mechanizmów certyfikacji (art. 44–50);
– przyjęcie założenia, zgodnie z którym podmioty prowadzące działalność w wielu państwach UE podlegać mają zasadniczo jurysdykcji jednego organu nadzorczego z tego państwa, w którym zlokalizowana jest ich główna jednostka organizacyjna na Unię (tzw. zasada *one-stop-shop*);
– zastąpienie dotychczasowej Grupy Roboczej Art. 29 dyrektywy 95/46/WE nowym organem – Europejską Radą Ochrony Danych (art. 68–76);
– ujednolicenie w skali UE oraz istotne wzmocnienie zasad odpowiedzialności w sytuacji naruszenia przepisów rozporządzenia, w szczególności wyposażenie organów nadzorczych (w tym GIODO) w możliwość nakładania administracyjnych kar pieniężnych (zob. dalsze uwagi);
– przyjęcie możliwości reprezentowania podmiotów danych przed właściwymi organami ds. ochrony danych oraz sądami przez organizacje o charakterze niezarobkowym (organizacje *non-profit*), które działają w dziedzinie ochrony danych osobowych (art. 80).

Z uwagi na skalę zmian wprowadzanych przez ogólne rozporządzenie w dalszej części artykułu szczegółowo przedstawione zostaną wybrane zagadnienia, które z perspektywy prowadzonej przez zakłady ubezpieczeń działalności mogą

budzić szczególne zainteresowanie, niejednokrotnie rodząc istotne zastrzeżenia i wątpliwości interpretacyjne. W kolejności przedstawione zostaną: przesłanka zgody podmiotu danych, problematyka związana z profilowaniem, przekazywanie danych w ramach grupy kapitałowej, w tym do państw trzecich, wreszcie – podstawowe zasady odpowiedzialności za naruszenie przepisów rozporządzenia.

3. Zgoda jako podstawa przetwarzania danych osobowych, w tym danych wrażliwych

Określenie wymogów w zakresie zgody, jako jednej z podstawowych – również w praktyce ubezpieczeniowej – przesłanek legalizujących operacje na danych osobowych, stanowiło istotne wyzwanie w trakcie prac nad projektem ogólnego rozporządzenia. Liczba zgłoszonych w tym zakresie przez zainteresowane strony (Komisję, Parlament Europejski, poszczególne państwa, organizacje branżowe itd.) poprawek, propozycji i pomysłów sprawiła, że **przepisy rozporządzenia dotyczące zgody budzą istotne wątpliwości interpretacyjne, niejednokrotnie pozostając ze sobą w sprzeczności, co utrudnia właściwe odczytanie oczekiwań unijnego prawodawcy w tym zakresie.** Zgodnie z przyjętą w rozporządzeniu definicją, zgoda osoby, której dane dotyczą stanowi *„dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych”* (art. 4 pkt 11). Fragment definicji odnoszący się do „wyraźnego działania potwierdzającego” (oraz wymogu wyrażenia zgody w formie określonego oświadczenia) skłania ku poglądowi, iż prawodawca unijny opowiedział się za modelem zgody *opt-in*, co jednak budzi pewne wątpliwości biorąc pod uwagę brzmienie motywów do rozporządzenia, które wydaje się dopuszczać również inne modele zgody (tj. zwrócenie uwagi na element zachowania, który „w danym kontekście” wskazuje na akceptację podmiotu danych)[5]. Z perspektywy krajowych ubezpieczycieli oczekiwanie zbierania zgód w modelu *opt-in* nie powinno jednakże rodzić problemów, biorąc pod uwagę, że definicja zgody funkcjonująca na podstawie ustawy o ochronie danych osobowych (art. 7 pkt 5) odpowiada temu modelowi zgody.

Wśród wymogów, jakie spełniać powinna na gruncie nowej regulacji zgoda, szczególne znaczenie nadano elementowi dobrowolności. Zgodnie z art. 7 ust. 4 rozporządzenia, przy ocenie, czy zgodę wyrażono w sposób dobrowolny należy wziąć pod uwagę, czy od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w sytuacji gdy przetwarzanie danych osobowych nie jest niezbędne do wykonania takiej umowy. Zastrzeżenie to budzi pewne

[5] Zgodnie z motywem 32, wyrażenie w ten sposób zgody może *„polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody”*.

wątpliwości konstrukcyjne, w sytuacji bowiem, gdy przetwarzanie danych jest niezbędne do wykonania umowy, podstaw do przetwarzania danych należy poszukiwać raczej w przepisie art. 6 ust. 1 lit. c), nie zaś w art. 6 ust. 1 lit. a) rozporządzenia. Ponadto, w świetle motywu 42, wyrażenie zgody nie będzie dobrowolne, jeżeli podmiot danych *„nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji"*. Wyraźne uprawnienie do cofnięcia zgody przewidziano w art. 7 ust. 3 rozporządzenia; co interesujące zastrzeżono tam również, że wycofanie zgody musi być równie łatwe jak jej udzielenie, co ma przeciwdziałać niepokojącym praktykom utrudniania podmiotom danych składania oświadczeń o wycofaniu zgody, w szczególności w środowisku Internetu.

W kontekście wymogu dobrowolności zwraca uwagę również motyw 43 rozporządzenia, który podaje w wątpliwość możliwość powoływania się na zgodę jako podstawę przetwarzania danych w sytuacji, w której istnieje *„wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach"*. Dodatkowo, zgodnie z brzmieniem tego motywu, zgody nie uważa się za dobrowolną, w sytuacji gdy *„nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne"*. Wbrew brzmieniu tego fragmentu rozporządzenia, **nie wydaje się, aby wymagał on zbierania odrębnych zgód na poszczególne czynności na danych**, dosłowna realizacja takiego wymogu prowadzić mogłaby bowiem do licznych absurdów. Pojęcie „czynności" (przetwarzania danych) stanowi termin nieostry i trudny z tego względu do jednoznacznej interpretacji, wydaje się jednak, iż jako odrębną czynność na danych można traktować np. zebranie danych, ich zapisanie w systemie informatycznym, przechowywanie (*hosting*) danych, anonimizację danych, zmianę czy usunięcie danych itd. W tym kontekście wymóg zbierania odrębnych zgód na poszczególne tego rodzaju czynności byłby niezwykle trudny do realizacji. Ponadto odmienny wniosek można wyprowadzić z brzmienia motywu 32, zgodnie z którym *„zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach*". Fragment ten sugeruje, że jedną zgodą (klauzulą zgody) objąć można różne, a nawet wszystkie, czynności na danych, jakie podejmowane są w określonym celu (celach).

Analiza przepisów rozporządzenia nie daje również jednoznacznej odpowiedzi czy, oraz ewentualnie w jakich przypadkach, **dopuszczalne jest łączenie w jednej klauzuli (w jednym oświadczeniu) zgód na przetwarzanie danych osobowych w różnych celach**, co dla praktyki obrotu, w tym w sektorze ubezpieczeniowym, ma szczególnie istotne znaczenie. Z motywu 32 wynika, że w przypadku, gdy przetwarzanie danych *„służy różnym celom"* zgoda powinna zostać udzielona *„na wszystkie te cele"*. Na tej podstawie nie sposób jednakże jednoznacznie przesądzić, czy jedna klauzula zgody może obejmować wszystkie te cele. Rozwiązanie to wydaje się jednakże sugerować użycie w motywie 32 terminu „zgoda" w liczbie pojedynczej (*„zgoda na wszystkie te cele"*).

Przepis art. 7 ust. 2 rozporządzenia wymaga – w sytuacji, gdy zgoda udzielana jest w pisemnym oświadczeniu, które dotyczy także innych kwestii – aby zapytanie o zgodę zostało przedstawione w sposób pozwalający wyraźnie odróżnić je od tych pozostałych kwestii. Dodatkowo, oświadczenie takie powinno mieć zrozumiałą i łatwo dostępną formę, zostać napisane jasnym i prostym językiem. W praktyce wymagać to będzie, w sytuacji gdy zgoda wyrażana jest np. w ramach wniosku ubezpieczeniowego, aby została ona wyraźnie odróżniona (w tym w formie graficznej) od innego rodzaju oświadczeń zbieranych w praktyce ubezpieczeniowej, związanych np. z akceptacją warunków ubezpieczenia. Biorąc pod uwagę, że rozporządzenie ogólne istotnie rozszerza katalog informacji, jakie administrator danych zobligowany jest podawać w przypadku zbierania danych od podmiotów, których dane dotyczą (art. 13 ust. 1 oraz ust. 2)[6], spełnienie powyższych wymogów związanych z formą i językiem komunikatów może być w praktyce utrudnione.

Zwrócić należy również uwagę na wątpliwość, jaka pojawia się w kontekście tych przepisów rozporządzenia, które posługują się kategorią zgody wyraźnej (ang. *explicit consent*). Uzyskanie kwalifikowanej „wyraźnej" zgody od podmiotu danych wymagane jest w przypadku przetwarzania szczególnych kategorii danych osobowych (tzw. danych wrażliwych, zob. art. 9 ust. 2 lit. a)), zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach (art. 22 ust. 2 lit. c)) oraz w związku z przekazywaniem danych osobowych do państw trzecich (art. 49 ust. 1 lit. a)). Biorąc pod uwagę, że z samej już definicji zgody wynika, iż jest to dobrowolne, szczególne, świadome i jednoznaczne (ang. *unambiguous*) oświadczenie woli podmiotu, którego dane dotyczą, oraz że powinno ono przybrać formę *„wyraźnego działania potwierdzającego"*, **nie jest do końca jasne, jakie dodatkowe warunki należy spełnić, aby zgoda była wyraźna.** Wydaje się jednak, iż biorąc pod uwagę motyw 32 preambuły do rozporządzenia, prawodawca unijny dążył do podkreślenia, iż w tych szczególnych sytuacjach wyłączone jest zbieranie zgody, która byłaby domniemana lub dorozumiana z oświadczenia woli o innej treści, np. którą można wywieść z określonego wyboru ustawień technicznych[7]. Wydaje się, że w praktyce zbieranie kwalifikowanej „wyraźnej" zgody od podmiotu danych powinno następować poprzez odebranie wyraźnego oświadczenia określonej treści, w szczególności poprzez podpisanie się przez zainteresowaną osobę pod takim oświadczeniem lub np. zaznaczenie stosownej opcji („okna") przy klauzuli zgody.

---

[6] Z reguły klauzule informacyjne towarzyszą klauzulom, za pomocą których zbierana jest zgoda podmiotów, których dane dotyczą; w praktyce klauzule te łączone są również w jedną klauzulę.

[7] Do wniosków takich prowadzi w szczególności analiza opinii Grupy Roboczej Art. 29 dyrektywy, *Opinion 15/2011 on the definitione of consent*, z 13 lipca 2011 r., WP 187, s. 25, na której to opinii prawodawca unijny w dużej mierze wzorował rozwiązania przyjęte w rozporządzeniu ogólnym.

4. Profilowanie w działalności ubezpieczeniowej na nowych zasadach

Liczne procesy biznesowe realizowane przez zakłady ubezpieczeń zakładają, w mniejszym lub większym zakresie, prowadzenie profilowania, rozumianego jako kategoryzowanie osób na podstawie różnych ich cech, zarówno „niezmiennych" (np. płeć, kolor oczu), jak również „zmiennych" (np. zachowanie, preferencje)[8]. W celu profilowania wykorzystywane są określone modele matematyczne, które pozwalają na tworzenie na podstawie danych, z reguły pochodzących z różnych źródeł, „sylwetek" klientów lub potencjalnych klientów, co pozwala zakładowi ubezpieczeniowemu na przygotowanie precyzyjnej, zindywidualizowanej oferty lub przeprowadzenie oceny ryzyka ubezpieczeniowego (tzw. *underwriting*). Jednocześnie stwarza to ryzyko po stronie podmiotów danych: zastosowanie modeli matematycznych nie pozwala bowiem na uwzględnienie skomplikowanych sytuacji życiowych, prowadzić może też do dyskryminacji lub innych niekorzystnych sytuacji (np. nieuzasadnionego podejrzenia prowadzenia działań na szkodę zakładu ubezpieczeń). W ramach działalności ubezpieczeniowej profilowanie może być również wykorzystywane w związku z zapobieganiem i zwalczaniem przestępczości ubezpieczeniowej, prowadzeniem działalności marketingowej, a także w kontekście zatrudnienia i oceny pracy. Wejście w życie rozporządzenia o ochronie danych osobowych **może skomplikować prowadzenie tego rodzaju operacji, a to z uwagi na szczególną regulację dotyczącą operacji profilowania w nowych unijnych ramach prawnych**.

Rozporządzenie wprowadza pojemną definicję profilowania (art. 4 pkt 4). Zgodnie z nią, profilowanie stanowi *„dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się"*. Przepis art. 22 ust. 1 ogólnego rozporządzenia wprowadza natomiast prawo podmiotu danych do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu (w tym na profilowaniu właśnie) oraz która to decyzja wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływa (np. skutkująca automatycznym odrzuceniem elektronicznego wniosku o objęcie ochroną ubezpieczeniową). Od zasady tej (zakazu) dopuszczono pewne odstępstwa, obejmujące trzy sytuacje (art. 22 ust. 2):

[8] J. Niklas, „Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji", dostępne pod adresem: http://www.ptpa.org.pl/public/files/publikacje/opinie/Opinia_profilowanie_w_kontek%C5%9Bcie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf [15.07.2016], s. 2.

1) decyzja taka jest niezbędna do zawarcia lub wykonania umowy pomiędzy osobą, której dane dotyczą, a administratorem danych (zakładem ubezpieczeń);
2) jest ona dozwolona prawem UE lub też prawem państwa członkowskiego, któremu podlega administrator i które przewiduje *„właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą”*,
3) decyzja opiera się na wyraźnej zgodzie podmiotu danych.

W tym kontekście dostrzec **można zasadniczą zmianę nowego stanu prawnego, porównując go z dotychczasową regulacją**. Operacje profilowania, które prowadzą do zautomatyzowanego podejmowania decyzji wywołujących wobec podmiotu danych skutki prawne lub wpływające w podobny sposób istotnie na podmiot danych, będą bowiem wymagały dla ich legalizacji oparcia na jednej z trzech, wskazanych wyżej podstaw. W tym też zakresie wyłączona została możliwość powoływania się na inne podstawy przetwarzania danych o charakterze generalnym, w szczególności na tzw. klauzulę uzasadnionych interesów administratora danych. Dodatkowo rozporządzenie wprowadza w zakresie operacji zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania, szczegółowe obowiązki obejmujące:

a) wdrożenie właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów podmiotu, którego dane dotyczą, przez co rozumieć należy w szczególności zapewnienie interwencji ludzkiej ze strony administratora danych[9], jak również zagwarantowanie jednostce prawa do wyrażenia własnego stanowiska oraz do zakwestionowania decyzji podjętej w sposób zautomatyzowany (art. 22 ust. 3 – co nie znajduje jednakże zastosowania w sytuacji objętej zakresem art. 22 ust. 2 lit. b));
b) uwzględnienie dodatkowych ograniczeń w sytuacji podejmowania tego rodzaju decyzji na podstawie tzw. danych wrażliwych (art. 22 ust. 4);
c) zastosowanie odpowiednich matematycznych lub statystycznych procedur profilowania, jak również wdrożenie środków zapewniających zmniejszenie ryzyka popełniania błędów oraz dyskryminacji osób fizycznych z uwagi m.in. na pochodzenie rasowe lub etniczne, stan genetyczny lub zdrowotny (motyw 71 preambuły).

Przyjęte na gruncie art. 22 rozporządzenia rozwiązanie potwierdza, iż **prawodawca unijny nie wprowadził generalnego zakazu stosowania technik opartych na profilowaniu, a jedynie istotne w tym zakresie ograniczenie, związane z zawężeniem możliwych podstaw prawnych dla przeprowadzania tego rodzaju operacji.** Co więcej, jak należy wnosić z przepisów rozporządzenia, wprowadzone obostrzenia nie dotyczą samego

[9] Nie w każdym przypadku zapewnienie czynnika ludzkiego będzie łatwe. Dotyczyć może to przykładowo dystrybucji mniej skomplikowanych produktów ubezpieczeniowych, oferowanych w kanale *direct* (w szczególności *on-line*) przy założeniu pełnej automatyzacji procesu (tj. przeprowadzenie oceny ryzyka na podstawie wprowadzonych w formularzu *on-line* danych, przedstawienie oferty oraz zawarcie umowy ubezpieczenia *on-line*).

tworzenia profili, lecz jedynie ich wykorzystania, tj. w sytuacji gdy operacje tego rodzaju prowadzić będą do podjęcia określonych decyzji wywołujących skutki prawne lub mających istotny wpływ na sytuację danej osoby fizycznej[10]. Tym samym stosowanie mechanizmów opartych na profilowaniu, w tym również w branży ubezpieczeniowej, w takim zakresie, w jakim nie będzie prowadzić do podejmowania określonych decyzji (tj. samo tworzenie profili), **będzie mogło znajdować oparcie również na innych podstawach prawnych, nie tylko tych ujętych przepisem art. 22 ust. 2**. Stanowisko to potwierdza również definicja profilowania przyjęta na gruncie rozporządzenia[11], a także brzmienie art. 21 ust. 1. Zgodnie z tym ostatnim przepisem, podmiot danych ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania danych osobowych opartego na podstawie ujętej w art. 6 ust. 1 lit. e) lub lit. f) rozporządzenia, w tym profilowania na podstawie tych przepisów. Potwierdza to, że samo tworzenie profili, o ile nie prowadzi do podejmowania decyzji wywołujących skutki prawne lub w podobny sposób oddziałujących na jednostkę, może być oparte na innych podstawach prawnych, w tym na tzw. klauzuli uzasadnionych interesów administratora (art. 6 ust. 1 lit. f) rozporządzenia).

Ogólne rozporządzenie kładzie również duży nacisk na wzmocnienie transparentności w związku z prowadzeniem operacji profilowania. Wymagane jest w związku z tym poinformowanie osób, których dane dotyczą, nie tylko o samym fakcie zautomatyzowanego podejmowania decyzji wykorzystującego profilowanie, lecz również o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (tak przepisy art. 13 ust. 2 lit. f), art. 14 ust. 2 lit. g) oraz art. 15 ust. 1 lit. h)). Brzmienie przepisów statuujących obowiązek informacyjny, interpretowanych w związku z art. 22 ust. 1, mogłoby skłaniać do wniosku, że nie jest konieczne informowanie o samym fakcie tworzenia profili, a jedynie o profilowaniu, które wykorzystywane jest do zautomatyzowanego podejmowania decyzji. Z interpretacją taką nie można jednak się zgodzić, **obowiązek informowania o samym tworzeniu profili (co zakłada przetwarzanie danych osobowych) wyprowadzić należy bowiem z ogólnego obowiązku informacyjnego (art. 13 ust. 1 lit. c) rozporządzenia)**.

---

[10] Rozwiązanie takie, jeszcze na etapie prac legislacyjnych, krytykowała m.in. Grupa Robocza Art. 29 dyrektywy; zob. „Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation", z 13 maja 2013 r., dostępny pod adresem: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf [28.07.2016], s. 3.

[11] Porównując przedmiotową definicję z definicją przyjętą w Rekomendacji Komitetu Ministrów państw członkowskich (Rady Europy) w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, CM/Rec (2010) 13 (polskie tłumaczenie dostępne pod adresem: www.giodo.gov.pl/plik/id_p/2155/j/pl/ [15.07.2016]), zwraca uwagę brak uwzględnienia w definicji przyjętej w rozporządzeniu aspektu związanego z podejmowaniem decyzji. Rekomendacja definiuje bowiem tworzenie profili (profilowanie) jako *„automatyczną technikę przetwarzania danych polegającą na przypisaniu danej osobie „profilu" w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw"* (pkt 1e)).

5. Przekazywanie danych w grupie kapitałowej, w tym do państw trzecich

Postępująca globalizacja, przejawiająca się m.in. wzrostem współpracy w ramach międzynarodowych grup kapitałowych (w tym grup finansowych, do których należą zakłady ubezpieczeń), spowodowała, że problematyka ta spotkała się ze stosunkowo dużym zainteresowaniem ze strony unijnego prawodawcy w ramach prac nad ogólnym rozporządzeniem. Zakładać należy, że liczne z przyjętych na gruncie rozporządzenia rozwiązań wpływać będą na usprawnienie tego rodzaju współpracy, wymagającej ponadgranicznego przekazywania danych osobowych. Na szczególną uwagę w tym zakresie zasługuje motyw 48 rozporządzenia, zgodnie z którym administratorzy, którzy są częścią grupy przedsiębiorstw (grupy kapitałowej) *„mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników”*. **Może to pozwalać m.in. na tworzenie scentralizowanych baz danych w europejskiej centrali korporacji i przekazywanie do nich danych osobowych z obszaru HR, jak również danych klientów zakładów ubezpieczeń**, bez konieczności poszukiwania dodatkowych podstaw dla takich operacji w przepisach ogólnego rozporządzenia (w szczególności w postaci zgody podmiotów danych). Nie oznacza to jednak, że dopuszczalne będzie niczym nieskrępowane przekazywane danych osobowych w ramach grup kapitałowych. Operacje takie wymagają bowiem uwzględniania również regulacji w zakresie ochrony tajemnicy ubezpieczeniowej (w szczególności w przypadku przekazywania danych klientów), jak również – w przypadku przekazywania danych poza obszar Unii Europejskiej – uwzględnienia rozwiązań dotyczących operacji transferów danych do państw trzecich. Jednoznacznie potwierdza to motyw 48, zgodnie z którym zasada w nim przyjęta pozostaje *„bez wpływu na ogólne zasady przekazywania danych osobowych w ramach grupy przedsiębiorstw przedsiębiorstwu mieszczącemu się w państwie trzecim”*.

Rozdział V rozporządzenia **przewiduje dalsze usprawnienia w zakresie przekazywania danych w ramach grup kapitałowych, prowadzących działalność w szerszej, niż wyłącznie europejska, skali** (transfery danych do państw trzecich). W tym zakresie na uwagę zasługuje w szczególności przyjęcie wyraźnej regulacji dotyczącej wiążących reguł korporacyjnych (ang. *Binding Corporate Rules*), którym poświęcono odrębny, rozbudowany przepis (art. 47). Powinno to usunąć szereg problemów i wątpliwości związanych z wykorzystaniem przedmiotowego instrumentu, w tym na powszechne jego uznanie w skali UE. Usprawnieniu operacji ponadgranicznych transferów danych służyć powinno również wyraźne zastrzeżenie, zgodnie z którym posłużenie się takimi instrumentami, jak (zatwierdzone) wiążące reguły korporacyjne lub standardowe klauzule umowne (w rozporządzeniu określane mianem „standardowych klauzul ochrony danych”) przyjęte przez Komisję lub przez krajowy organ ds. ochrony danych (co wymaga jednakże dodatkowego zatwier-

dzenia przez Komisję), nie wymaga *„uzyskania specjalnego zezwolenia ze strony organu nadzorczego”*, tj. nie wymaga dodatkowej autoryzacji na poziomie krajowym, np. w postaci zgody GIODO, o której mowa w art. 48 ustawy o ochronie danych osobowych. Nowymi, nieznanymi dotychczas instrumentami transferowymi, będą również: zatwierdzone kodeksy postępowania (kodeksy dobrych praktyk), przyjmowane zgodnie z art. 40 rozporządzenia oraz mechanizmy certyfikacji (tzw. znaki jakości i oznaczenia, np. określone pieczęcie, ang. *data protection/privacy seals*), zatwierdzane zgodnie z art. 42 rozporządzenia. Skorzystanie z dwóch ostatnich instrumentów wymaga jednakże dodatkowo zastosowania *„wiążących i egzekwowalnych zobowiązań administratora (…) w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą”* (tak wyraźnie art. 46 ust. 2 lit. e) i f)), w sposób jednak nie do końca poprawny redakcyjnie, a przez to budzący pewne wątpliwości). Na uwagę zasługuje również w tym zakresie wprowadzenie dodatkowej przesłanki uprawniającej do transferu danych, w postaci tzw. uzasadnionych interesów eksportera danych (art. 49 ust. 1 akapit drugi). Wydaje się jednak, że praktyczne znaczenie tej ostatniej przesłanki będzie niewielkie, biorąc pod uwagę liczbę i charakter ograniczeń warunkujących możliwość skorzystania z niej (m.in. brak możliwości skorzystania z innych mechanizmów transferowych objętych przepisami art. 45 oraz art. 46; ograniczenie transferu do tego rodzaju operacji, które nie są powtarzalne, jak również takich, które dotyczą włącznie ograniczonej liczby podmiotów danych itd.).

6. Odpowiedzialność administracyjna (finansowa)

Wzmocnienie zasad odpowiedzialności administratorów danych oraz podmiotów przetwarzających, do jakiego doszło na skutek przyjęcia ogólnego rozporządzenia, przejawia się w szczególności w możliwości nakładania przez organy nadzorcze (w tym Generalnego Inspektora) administracyjnych kar pieniężnych. Rozporządzenie wprowadza dwie grupy naruszeń, dla których przewidziano następujące limity odpowiedzialności o charakterze finansowym:

1) karę pieniężną w wysokości do 10 000 000 euro lub – w przypadku przedsiębiorstw – w wysokości do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa, art. 83 ust. 4); kara w takiej wysokości może zostać nałożona np. w sytuacji naruszenia obowiązków związanych z ochroną danych w fazie projektowania lub związanych z bezpieczeństwem danych osobowych;
2) karę pieniężną w wysokości do 20 000 000 euro lub – w przypadku przedsiębiorstw – w wysokości do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa, art. 83 ust. 5); kara w takiej wysokości może zostać nałożona np. w sytuacji naruszenia podstawowych zasad przetwarzania danych, w tym warunków udzielenia przez podmiot danych zgody, bądź też naruszenia zasad związanych z przekazywaniem danych osobowych do państw trzecich.

Na organy nadzorcze poszczególnych państw członkowskich nałożono obowiązek zapewnienia, aby nakładane na podstawie rozporządzenia administracyjne kary pieniężne *„były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające”* (art. 83 ust. 1). Wśród kryteriów, jakie organ powinien brać pod uwagę podejmując decyzję o nałożeniu kary, jak również o jej wysokości, wymieniono (art. 83 ust. 2):

a) charakter, wagę i czas trwania naruszenia, z uwzględnieniem charakteru, zakresu oraz celu operacji przetwarzania danych, liczby poszkodowanych osób, których dane dotyczą, jak również takich czynników jak rozmiar poniesionej przez podmioty danych szkody;
b) umyślny lub nieumyślny charakter naruszenia;
c) działania podjęte przez administratora danych (podmiot przetwarzający) w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
d) wszelkie wcześniejsze naruszenia zasad ochrony danych osobowych ze strony administratora (podmiotu przetwarzającego);
e) współpracę z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
f) znaczenie mogą mieć również w tym kontekście osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty;
g) istotny może być także sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie podmiot zobowiązany zgłosił naruszenie (do czego obliguje go art. 33 rozporządzenia, wprowadzający powszechny – obejmujący również zakłady ubezpieczeń – obowiązek notyfikacji przypadków naruszeń ochrony danych osobowych).

7. Podsumowanie

Przyjęcie ogólnego rozporządzenia o ochronie danych osobowych oraz jego wejście w życie (co nastąpiło, zgodnie z art. 99 ust. 1 rozporządzenia, w dniu 24 maja 2016 r., rozpoczynając tym samym 2-letni okres dostosowawczy) otwiera nowy rozdział w podejściu do problematyki ochrony danych osobowych. Skala zmian, w szczególności w zakresie obowiązków nakładanych na zakłady ubezpieczeń (jako administratorów danych), wymagać będzie podjęcia istotnych inwestycji w wewnętrzną organizację ochrony danych, w szczególności w tych organizacjach, które dotychczas takimi inwestycjami nie mogły się pochwalić. Swoistą „klamrę” spinającą obowiązki administratorów stanowi zasada rozliczalności, która wymaga od podmiotów zobowiązanych podejścia proaktywnego, wdrożenia określonych procedur i polityk, czy nawet przyjęcia kompleksowego programu zapewnienia zgodności w zakresie ochrony danych osobowych (ang. *Data Protection Compliance Program*).

Procesu dostosowawczego nie ułatwia z pewnością sposób redakcji rozporządzenia, posługującego się dużą liczbą pojęć nieostrych, klauzul general-

nych (takich jak np. „wysokie ryzyko naruszenia praw lub wolności osób fizycznych", „rozsądne działania", zapewnienie „wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych", „przetwarzanie na dużą skalę szczególnych kategorii danych osobowych" itd.), jak również jego tłumaczenie na język polski, pozostawiające wiele do życzenia (prace nad rozporządzeniem prowadzone były bowiem w języku angielskim). Oczekiwać należy w związku z tym zaangażowania w procesy dostosowawcze (m.in. w kontekście interpretacji budzących wątpliwości przepisów) ze strony organów nadzorczych, jak również Grupy Roboczej Art. 29 dyrektywy 95/46/WE, a następnie – po jej przekształceniu – Europejskiej Rady Ochrony Danych. Pierwsze kroki w tym zakresie są zresztą już podejmowane: Generalny Inspektor powołał Komisję Ekspertów do spraw reformy prawa ochrony danych osobowych w Unii Europejskiej[12], natomiast ww. Grupa Robocza Art. 29 zapowiedziała, iż m.in. wyda stosowne wytyczne dotyczące takich zagadnień i obszarów, jak: prawo do przenoszenia danych, pojęcie „wysokiego ryzyka", mechanizmy certyfikacyjne, czy rola inspektora ochrony danych (odpowiednika administratora bezpieczeństwa informacji)[13]. Nie pozostaje nic innego jak śledzenie tych inicjatyw, ich pomoc w dostosowaniu zakładów ubezpieczeń do nowych ram prawnych może być bowiem nieoceniona.

Damian Karwala
Radca prawny, współpracujący z kancelarią prawną
DLA Piper Wiater sp. k., członek zespołu
Intellectual Property and Technology

Bibliografia

„Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation", z 13 maja 2013 r., dostępny pod adresem: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf [28.07.2016].

Nikłas J. 2016. „Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji", dostępne pod adresem: http://www.ptpa.org.pl/public/files/publikacje/opinie/Opinia_profilowanie_w_kontek%C5%9Bcie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf [15.07.2016].

Rekomendacja Komitetu Ministrów państw członkowskich (Rady Europy) w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, CM/Rec (2010) 13 (polskie tłumaczenie dostępne pod adresem: www.giodo.gov.pl/plik/id_p/2155/j/pl/ [15.07.2016]).

[12] Źródło: http://www.giodo.gov.pl/560/id_art/9410/j/pl/ [30.06.2016].

[13] Zob. „Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)", z 2 lutego 2016 r., WP 236, dostępny pod adresem: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf [30.06.2016].

„Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)", z 2 lutego 2016 r., WP 236, dostępny pod adresem: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf [30.06.2016].

The Impact of the Regulation on the Protection of Personal Data on the Activity of Insurance Companies – Selected Issues

The adoption of the Regulation (EU) 2016/679 of 27 April 2016 on data protection ended the four-year work on the reform of the EU legal framework regulating the protection of personal data. The provisions of the regulation are intended to replace Directive 95/46/EC and, generally, the Personal Data Protection Act. They will also affect the interpretation of the sector-specific regulation, namely the Insurance and Reinsurance Activity Act.
From the perspective of insurance undertakings certain solutions are of particular importance, including those that refer to the basis for data processing in the form of the data subject's consent; profiling, particularly leading to an automated decision making; the transfer of personal data within corporate groups, including the third countries; and finally, the basic principles of liability for breach of the provisions of the regulation due to the introduction of possible financial penalties to be imposed by supervisory authorities.

Keywords: regulation on the protection of personal data, the data subject's consent, profiling, administrative (financial) responsibility of the data controller.