RODO do poprawki

Niedługo minie 6 lat stosowania RODO, a kilka tygodni temu wybrano nowego Prezesa Urzędu Ochrony Danych Osobowych. Jest to zatem znakomity moment, by wrócić do jednego z kluczowych problemów RODO wciąż wymagających działania, czyli do wyjaśnienia błędów w tłumaczeniu Rozporządzenia, o czym wspomniałam w numerze 1/2023 Domeny.

Joanna Karczewska

absolwentka Wydziału Elektroniki PW z ponad 40-letnim doświadczeniem w informatyce. Jako certyfikowany audytor systemów informatycznych – CISA – specjalizuje się w audytach informatycznych w jednostkach sektora finansów publicznych. Pełni także funkcję inspektora ochrony danych w placówkach oświatowych. Jako Expert Reviewer uczestniczyła w opracowaniu metodyk COBIT5 i COBIT 2019, ITAF 4th Edition oraz publikacji ISACA dotyczących Digital Trust Ecosystem Framework. Bierze udział w konsultacjach aktów prawnych dotyczących bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych osobowych, również na forum Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP. Uznana w 2022 roku za jedną z Europe's Top Cyber Women. Ekspert Najwyższej Izby Kontroli.

Problem jest znany od dnia opublikowania RODO. Wiele osób, mając wątpliwości, wolało w swojej pracy bazować na wersji oryginalnej, czyli angielskiej. Ambitni zestawiali dla porównania kilka wersji językowych.

Znając biegle języki angielski i francuski, też tak zrobiłam, dorzucając wersję hiszpańską. Najbardziej zaintrygowało mnie przetłumaczenie *documented instructions* na „udokumentowane polecenie" w artykule 28 Podmiot przetwarzający. Przypomnę zapis z ust. 3: „... podmiot przetwarzający: a) przetwarza dane osobowe **wyłącznie na udokumentowane polecenie administratora ...**" (w oryginale the processor: (a) processes the personal data **only on documented instructions from the controller**).

Pracując wiele lat w informatyce, zrozumiałam jednoznacznie, że wszelkie wymagania nazwane instrukcjami, dotyczące przetwarzania danych osobowych, administrator ma przekazywać procesorowi / podmiotowi przetwarzającemu tylko i wyłącznie na piśmie. Wymagania mogą dotyczyć chociażby częstotliwości wykonywania kopii zapasowych i miejsc ich przechowywania. Zajrzałam do *Słownika języka polskiego PWN* (https://sjp.pwn.pl) i dowiedziałam się, że instrukcja to „zbiór przepisów ustalających sposób postępowania w jakiejś dziedzinie"; także „dokładne pouczenie, wskazówka", zaś polecenie to „wypowiedź nakazująca komuś wykonanie jakiejś czynności". Zwracam uwagę na słowo „wypowiedź".

Europa precyzuje

Dla potwierdzenia mojej interpretacji sięgnęłam do wytycznych organów nadzorczych państw UE. Znakomite wyjaśnienie znalazłam w poradniku „Smernice Informacijskega pooblaščenca o (pogodbeni) obdelavi osebnih podatkov" (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_pogodbeni_obdelavi_web.pdf), wydanym przez słoweński organ Informacijski Pooblaščenec. Czytamy „ […] instrukcje mogą obejmować dopuszczalne i niedopuszczalne przetwarzanie danych osobowych, bardziej szczegółowe procedury, metody ochrony danych itp.". Zapoznałam się także z Wytycznymi 07/2020 dotyczącymi pojęć administratora i podmiotu przetwarzającego zawartych w RODO, wydanymi przez Europejską Radę Ochrony Danych (https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_pl.pdf). Stosowny zapis dotyczący art. 28 ust. 3 lit. a) brzmi: „116. Konieczność określenia tego obowiązku wynika z faktu, że podmiot przetwarzający przetwarza dane w imieniu administratora. Administratorzy muszą przekazywać podmiotom przetwarzającym instrukcje dotyczące każdej czynności przetwarzania. Takie instrukcje mogą obejmować dopuszczalne i niedopuszczalne sposoby przetwarzania danych osobowych, bardziej szczegółowe procedury, sposoby zabezpieczania danych itd. Podmiot przetwarzający nie może wykraczać poza instrukcje przekazane przez administratora. Podmiot przetwarzający może jednak sugerować elementy, które – jeśli zostaną zaakceptowane przez administratora – staną się częścią wydanych instrukcji".

Problem zbagatelizowany

W maju 2018 r., po opublikowaniu corrigendum do RODO, zgłosiłam kolejne niezbędne poprawki tłumaczenia Rozporządzenia do wskazanego Wydziału Jakości Regulacji Służby Prawnej Sekretariatu Generalnego Rady UE. Zaproponowałam m.in. zmianę na: a) przetwarza dane osobowe wyłącznie według udokumentowanych instrukcji administratora. Zwróciłam uwagę, że słowa „instrukcje" użyto w Rozporządzeniu (We) Nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

> *W 2021 r., czyli po trzech latach analizy, otrzymałam następującą odpowiedź: please be informed that after examination of your request and* ***consultations with competent Polish authorities*** *we came to a conclusion that the Polish version of the Regulation (EU) 2016/679 needs to be corrected as far as Article 82(2) is concerned and that other points raised in your message didn't warrant a corrigendum.*

Problem ukarany

Prawnicy przyjęli literalną interpretację art. 28 ust 3. lit. a) bez żadnego dodatkowego wyjaśnienia i powtarzają ją jak mantrę. Najlepszym przykładem ich podejścia jest kara administracyjna w wysokości 100 tys. zł nałożona w 2021 r. przez Prezesa UODO (https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020) na Krajową Szkołę Sądownictwa i Prokuratury (KSSIP).

Dla przypomnienia: incydent polegał na uzyskaniu nieupoważnionego dostępu do kopii bazy danych witryny szkoleniowej KSSIP powstałej w trakcie testowej migracji do nowej platformy szkoleniowej. Naruszenie dotyczyło ponad 50 tys. osób, użytkowników podlegających szkoleniu ustawicznemu, w tym aplikantów sędziowskich i prokuratorskich, sędziów, prokuratorów, asesorów, referendarzy, asystentów oraz pracowników sądów, a także osób prowadzących zajęcia w KSSiP, których dane osobowe zgromadzono na platformie szkoleniowej Szkoły. Kara została nałożona m.in. za powierzenie przetwarzania danych osobowych **bez zawarcia w umowie zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora**.

Jak wynika z uzasadnienia, umowa główna wprawdzie zawierała zapis *„[…] zgłoszenia usterek związanych z usługami hostingowymi, w tym ich niedostępność, dokonywane będą pisemnie, faksem lub pocztą elektroniczną"*, jednak w ocenie Prezesa UODO wskazane postanowienie umowy było niewystarczające. Umowa powierzenia zawarta z podmiotem przetwarzającym powinna zawierać przynajmniej ogólne sformułowanie zobowiązujące podmiot przetwarzający do działania wyłącznie na udokumentowane polecenie administratora. Pracownicy KSSiP nie mieli pełnej świadomości,

jak kształtują się prawa i obowiązki pomiędzy administratorem a podmiotem przetwarzającym, wynikające z umowy, zaś administrator kilkukrotnie oczekiwał wykonywania zadań wykraczających poza jej zakres. Jedynie na udokumentowane polecenie administratora podmiot przetwarzający może dokonywać ingerencji w zakresie wynikającym z charakteru świadczonych usług i zawartej umowy.

Sprawa była bardzo głośna. Media rozpisywały się o niej, a w jej wyjaśnienie zaangażowano wiele ważnych instytucji. Zastanawia, dlaczego szkoła edukująca prawników sama nie znała prawa. A może go nie rozumiała, bo zabrakło dodatkowych właściwych praktycznych wytycznych i objaśnień zapisów RODO, także dotyczących pojęcia „udokumentowane polecenie".

Problem powielany

Skoro konsekwencje braku formułki wymaganej przez Prezesa UODO w umowie powierzenia mogą być bolesne dla administratora, postanowiłam sprawdzić, jakie zapisy zawierają przyjęte i proponowane kodeksy postępowania, które mają pomagać we właściwym stosowaniu RODO.

Problem wyjaśniony?

Pod koniec 2023 r. Prezes Urzędu Ochrony Danych Osobowych nałożył 100 tys. zł kary na Ministra Zdrowia za ujawnienie w jednym z serwisów społecznościowych danych o stanie zdrowia lekarza pozyskanych z e-recepty wystawionej pro auctore. Sprawa była wyjątkowo głośna.

Wiele ciekawych informacji o naruszeniu i jego skutkach zawarto w uzasadnieniu nałożonej kary (https://www.uodo.gov.pl/decyzje/DKN.5131.32.2023).

Okazuje się, że po incydencie Minister zlecił przeprowadzenie audytu w Centrum e-Zdrowia, które odpowiada za organizację i prawidłowe funkcjonowanie Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych (P1) obejmującej usługę e-recepta. W raporcie z audytu znalazły się m.in. następujące cytowane ustalenia:

- polityka bezpieczeństwa danych osobowych obowiązująca w instytucji odwołuje się do nieaktualnych przepisów i stosowane jest stare podejście do ochrony danych osobowych;

W Kodeksie dla małych placówek medycznych, przyjętym w grudniu 2022 r., jedynie powielono treść art. 28.

W Kodeksie dla szpitali, przyjętym w grudniu 2023 r., w ogóle nie pojawia się „udokumentowane polecenie". Z kolei w projektach kodeksów złożonych do zatwierdzenia (https://uodo.gov.pl/pl/426/1109):

- **dla doradców podatkowych „udokumentowane polecenie" pojawia się dwa razy: w punkcie 6.19.1. jako cytat art. 28 ust. 3 lit. a) oraz we wzorze umowy powierzenia przetwarzania jako zapis: „Podmiot przetwarzający będzie przetwarzał dane osobowe wyłącznie na udokumentowane polecenie Podmiotu powierzającego. Udokumentowane polecenie może stanowić w szczególności niniejsza Umowa. Inne polecenia będą mogły być kierowane do Podmiotu przetwarzającego wyłącznie w formie …….";**
- **dla firm badania opinii i rynku formułki nie ma ani w projekcie kodeksu, ani w załączniku nr 5 (umowa powierzenia przetwarzania danych osobowych);**
- **dla centrów handlowych – nie ma żadnego zapisu (w wersji z dnia 29.06.2020 r.)**
- **dla biobanków – nie ma żadnego zapisu;**
- **dla branży hotelarskiej – zawarto tylko zapis „Powierzenie przetwarzania danych osobowych to sytuacja, w której inny podmiot przetwarza dane osobowe w imieniu administratora wypełniając jego polecenia. Podmiot przetwarzający przetwarza dane osobowe w określonym przez administratora celu".**

Przypomnę, że według Cambridge Dictionary: *code of conduct to set of rules that members of an organisation or people with a particular job or position* ***must follow***. Zatem kodeksy postępowania znakomicie nadają się do wyjaśnienia, co w praktyce oznacza „udokumentowane polecenie" administratora dla podmiotu przetwarzającego. Na razie nie precyzują.

- wymagana jest zmiana Porozumienia przez Centrum wraz z Ministerstwem Zdrowia w części dotyczącej **wydawania poleceń** przez Ministra Zdrowia w taki sposób, aby ewentualne polecenia wydawane były w trybie oficjalnym i zawierały sformułowanie „polecenie" (zamiast za pomocą poczty elektronicznej) oraz wprowadzenie zakazu stosowania innych kanałów komunikacji nieokreślonych w Porozumieniu.

Czy w sformułowaniu „wydawanie poleceń" chodzi o udokumentowane polecenie z art. 28 ust. 3 lit. a)? Tylko dostęp do samego raportu z audytu by to wyjaśnił.

Problem upoważniony

Ciąg dalszy zamieszania jest związany z artykułem 29 RODO, który dla jasności przytoczę w wersji oryginalnej: *The processor and any person acting under the **authority** of the controller or of the processor, who has access to personal data, shall not process those data **except on instructions from the controller**, unless required to do so by Union or Member State law* i w wersji polskiej: „Podmiot przetwarzający oraz każda osoba działająca z **upoważnienia** administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je **wyłącznie na polecenie administratora**, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego".

> *Otóż według prawników specjalizujących się w RODO owo upoważnienie i owo polecenie są tożsame.*

W poradniku wydanym w 2021 r. autor napisał m.in. „uprawnienie do przetwarzania danych tworzone jest dwuetapowo, przez upoważnienie i polecenie" oraz „przez nieuprawniony dostęp do danych przechowywanych należy rozumieć dostęp bez upoważnienia i bez polecenia administratora lub za upoważnieniem, ale bez polecenia administratora, lub bez upoważnienia podmiotu przetwarzającego i bez polecenia administratora, lub bez upoważnienia administratora, lub bez polecenia podmiotu przetwarzającego". Z kolei w innym poradniku wydanym pod koniec 2023 r. jego kolega po fachu stwierdził, że „*upoważnienie do przetwarzania danych osobowych to obecnie nie wymóg czysto biurokratyczny, lecz element systemu zabezpieczenia danych osobowych, którego istotę można sprowadzić do jednego: każdy, kto przetwarza dane, może to robić wyłącznie na polecenie administratora lub przetwarzającego, a wdrożenie systemu upoważnień ma to zapewnić*". Świadomie pomijam nazwiska, by nie narażać panów na różne komentarze i zalecam im refleksję. Oraz rozmowę z fachowcami od bezpieczeństwa informacji.

Problem z rzetelnością

W czasie posiedzenia Komisji Sprawiedliwości i Praw Człowieka 23 maja 2023 r. poprzedni Prezes UODO, Jan Nowak, zwrócił uwagę na inną – jego zdaniem – wątpliwość dotyczącą tłumaczenia RODO. Jego wywód dotyczył zapisu artykułu 5 Zasady dotyczące przetwarzania danych osobowych, który brzmi:

1. *Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, **rzetelnie** i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, **rzetelność** i przejrzystość")*, zaś w wersji angielskiej: 1. *Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, **fairness** and transparency')*.

Jak stwierdził Prezes: „Wydawałoby się, że ten zapis jest bardzo czytelny i wszyscy go rozumieją. Nic bardziej mylącego. Chodzi o to słowo **rzetelnie**. Dlaczego? To jest tłumaczenie RODO na język polski, ale szanowni państwo, RODO obowiązuje w 27 państwach europejskich, które mają różne języki i w związku z tym musiało być przetłumaczone na te języki. Tak się składa, że nasze tłumaczenie słowa **rzetelnie** jest absolutnie niewłaściwe, ale jest i u nas funkcjonuje. Co nie znaczy, że sądy mają sądzić tak, jak wskazuje tłumaczenie. W całej Europie, w każdym kraju europejskim należy sądzić i interpretować RODO identycznie. Tu nie ma odstępstw. Posłużę się przykładem niemieckim. To jest **rzetelny** wzór. Gdyby u Niemców było rzetelnie, to by było: *ehrlich*. Niemcy mają takie słowo, odpowiednik polskiego sformułowania rzetelnie. Ale w tłumaczeniu niemieckim jest: *nach treu und glauben*, co znaczy: w dobrej wierze". I dodał: „... po angielsku będziemy mieli słowo: ***fairly***, czyli bardziej idzie w kierunku – uczciwie, po francusku: ***loyal***. My mamy „**rzetelnie**". Jak coś się uda popsuć, to chociaż tłumaczenie".

Nie znam języka niemieckiego, znam angielski. Nie rozumiejąc, na czym polega „popsucie" w tym przypadku, dla pewności sięgnęłam do *Wielkiego Słownika Angielsko-Polskiego*. Według profesora Jana Stanisławskiego słowo „fairly" jako przysłówek oznacza:

1. sprawiedliwie; słusznie; bezstronnie
2. uczciwie; rzetelnie

Zatem użycie słowa „rzetelnie" jest uzasadnione i bardziej właściwe niż „w dobrej wierze".

Z wypowiedzi Prezesa UODO wynika, że nigdy nie zgłosił zmiany do wspomnianego dyrektoriatu Rady Unii Europejskiej. O swoim zastrzeżeniu nigdy nie napisał w biuletynie czy newsletterze wydawanym przez Urząd dla Inspektorów Ochrony Danych (przejrzałam wszystkie numery). Natomiast przyznał publicznie, że tłumaczenie RODO zostało popsute. Cieszę się, że nie tylko ja widzę problem.

Temat polecenia czy poleceń administratora dla podmiotu przetwarzającego i jego/ich dokumentowania wraca jak bumerang. Zatem czas najwyższy na corrigendum polskiej wersji RODO oraz na jasne i konkretne polskie wytyczne wyjaśniające, co w praktyce pomysłodawcy RODO mieli na myśli i jakie jest stanowisko Prezesa UODO.