Przedmowa

Zagadnienia związane z ochroną danych osobowych w sektorze ochrony zdrowia stały się tematem bardzo ożywionej dyskusji w związku z trwającą od 2012 r. reformą prawa ochrony danych w UE. W trakcie prac nad RODO kwestie ochrony danych o zdrowiu oraz ich współistnienie z innymi danymi osobowymi niejednokrotnie spędzały sen z oczu nie tylko przedstawicielom sektora ochrony zdrowia, lecz także wszystkim pracującym nad nowym rozporządzeniem unijnym – RODO. Co prawda, **w RODO harmonizacji uległy przepisy ogólne i nie ma wątpliwości, że wszystkie ogólne zasady RODO odnoszą się do wszystkich działań dotyczących przetwarzania danych dotyczących zdrowia. Samo RODO wyróżnia dane dotyczące zdrowia jako szczególny rodzaj danych.** Poza sporem pozostaje jednak również fakt, że dane medyczne mogą podlegać innym szczególnym przepisom, które nie zostały w całości uchylone, a normy z nich wynikające mogą wchodzić w kolizję z RODO. Z tego też powodu Europejska Rada Ochrony Danych (EROD) nie zajęła się dotąd przygotowaniem jakichkolwiek wytycznych odnoszących się do danych dotyczących zdrowia, pozostawiając poszczególnym organom nadzorczym – popularnie wciąż określanym jako organy ochrony danych – zadanie rozpoznania pól, na których taki konflikt norm – lub przynajmniej ich wzajemne przenikanie – może wystąpić.

Mimo wszystkich różnic pomiędzy systemami prawnymi państw członkowskich UE oraz pomiędzy rozwiązaniami organizacyjnymi leżącymi u podstaw systemu ochrony zdrowia w tych krajach, w każdym z nich – w momencie rozpoczęcia pełnego stosowania RODO – doszło do zastąpienia rozporządzeniem ustaw regulujących dotąd materialną stronę ochrony danych osobowych i wdrażających dyrektywę 95/46/WE Parlamentu i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L 1995 Nr 281, s. 31 ze zm.; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355). Tym samym wszelkie rozważania związane z reformą prawa ochrony danych osobowych w UE w oczywisty sposób dotyczą również tych danych, które traktowane są jako dane o stanie zdrowia, w tym tzw. danych medycznych. Warto jednocześnie pamiętać, że RODO w podobny sposób reguluje bardzo szeroki zakres innych danych związanych z działaniem systemu ochrony zdrowia. W motywie 35 RODO wyraźnie wskazano, że do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie jej zdrowia fizycznego lub psychicznego. Podkreślono, że choć *clue* stanowią tu informacje zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej określone w dyrektywie Parlamentu Europejskiego i Rady Nr 2011/24/UE z 9.3.2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.Urz. UE L 88 z 2011 r., s. 45) (numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych) oraz informacje pochodzące z badań laboratoryjnych lub lekarskich (w tym danych genetycznych i danych z próbek biologicznych), to w podobny sposób należy traktować również wszelkie informa-

cje o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby niezależnie od ich źródła (lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne *in vitro*). Wskazano jednocześnie, że podstawy prawne do przetwarzania takich danych muszą uwzględniać wyjątki (przewidziane w prawie unijnym lub w prawie państwa członkowskiego) uzasadnione interesem publicznym w zakresie bezpieczeństwa, monitorowania i ostrzegania zdrowotnego, zapobiegania chorobom zakaźnym i innym poważnym zagrożeniom zdrowotnym. Taki wyjątek może być przewidziany ze względu na cele zdrowotne, w tym związane ze zdrowiem publicznym oraz zarządzaniem usługami opieki zdrowotnej, w szczególności zapewnianiem jakości i ekonomiczności procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych. Wszystkie te zastrzeżenia oddają złożony charakter przetwarzania danych w ochronie zdrowia i wielowątkowość kwestii dotyczących przetwarzania danych związanych ze zdrowiem w systemach informacyjnych wykorzystywanych w ochronie zdrowia. Autorzy niniejszego opracowania wskazują na podobieństwa i różnice pomiędzy różnymi metodami przetwarzania danych i różnymi środowiskami, w których przetwarzanie następuje. Rozważania mają zastosowanie do systemów informatycznych (i szerzej systemów informacyjnych) używanych w ochronie zdrowia, a tworzonych w obecnej chwili w większości krajów UE.

Krajobraz legislacyjny, w którym działają owe systemy, jest jednak znacznie szerszy niż samo RODO. Do najistotniejszych aktów prawnych, które należy brać pod uwagę przy wykładni RODO, należą – poza OchrDanychU, która uzupełnia – a niekiedy wprowadza w życie rozwiązania RODO – regulacje wprost skierowane do rynku medycznego, takie jak PrPacjRPPU czy SystInformOchrZdrU oraz rozporządzenia wykonawcze do tej ustawy. Ogólne rozporządzenie o ochronie danych jest bowiem tylko narzędziem służącym temu, aby ochrona prywatności i bezpieczeństwa informacji była prawidłowa dla systemu ochrony zdrowia. Jest to więc tylko jeden z komponentów uzupełniających akty wprost regulujące rynek usług medycznych i danych w tych usługach wykorzystywanych.

Książka, którą otrzymują Państwo do rąk, z jednej strony, omawia rozwiązania wprowadzone przez RODO oraz przez OchrDanychU, z drugiej zaś, odnosi się do przepisów szczególnych stworzonych dla systemu ochrony zdrowia w Polsce, uzupełniając je rozważaniami dotyczącymi przepisów ogólnych odnoszących się do informatyzacji. Istotne znaczenie będzie miała więc InformPodPublU – tzw. ustawa o informatyzacji administracji – wraz z aktami wykonawczymi (przede wszystkim Krajowymi Ramami Interoperacyjności) oraz KPA w tym zakresie, w jakim odnosi się on do czynności administracyjnych podejmowanych w postaci elektronicznej.

Wzajemne przenikanie się wszystkich tych przepisów tworzy skomplikowaną, ale w miarę logiczną całość, którą w praktyce muszą się posługiwać wszystkie podmioty zajmujące się ochroną zdrowia w Polsce. Nie ma możliwości wyspecjalizowania się tylko w jednej z tych dziedzin. Podmiot prowadzący działalność medyczną musi sprawnie wykonywać obowiązki, ale też realizować swoje własne uprawnienia wynikające z wszystkich tych przepisów.

Podmioty ochrony zdrowia muszą również wyraźnie rozróżniać, w jakiej roli występują w poszczególnych operacjach przetwarzania danych osobowych. Każda instytucja działająca w systemie ochrony zdrowia pełni bowiem na co dzień różne role z punktu widzenia prawa ochrony danych osobowych. Może być administratorem danych pacjentów, administratorem danych osób zatrudnionych w systemie ochrony zdrowia, ale może być również procesorem – przetwarzającym dane osobowe na potrzeby innych administratorów. Administratorem danych jest w tym rozumieniu każdy podmiot, który decyduje o celach i sposobach przetwarzania danych. Podmiotem takim może być szpital jako całość, jednostka naukowa, uczelnia, wydział lub instytut, w zależności od tego, na jakim poziomie organizacyjnym podejmowane są decyzje dotyczące celów i sposobu przetwarzania danych.

Administratorem danych w ochronie zdrowia może być w końcu indywidualny lekarz prowadzący indywidualną działalność medyczną. Do podobnej sytuacji może również dojść, gdy lekarz pracuje w większej instytucji, lecz *de facto* ma samodzielną pozycję – np. lekarz orzecznik zajmujący się medycyną pracy bądź lekarz pracujący dla instytucji ubezpieczeniowej i wykonujący działania na jej potrzeby. W tym ostatnim przypadku nie wszystkie dane pochodzące z oceny stanu zdrowia pacjenta będą danymi, których administratorem będzie ubezpieczyciel.

Rola administratora danych w tym przypadku nie jest jednorodna. Jest to bowiem rola tego, kto leczy pacjenta, tego, kto sprawuje opiekę nad pacjentem, tego, kto monitoruje zachowanie pacjenta nie tylko w trakcie przebywania przez niego na terenie podmiotu leczniczego, ale również zachowanie przed rozpoczęciem leczenia oraz po jego zakończeniu. Inaczej będzie wyglądała też rola takiego podmiotu wtedy, gdy wykonywać będzie zadania związane z archiwizacją danych pacjentów leczonych w przeszłości. Podmioty te występują jednak również w roli pracodawcy bądź w roli uczestnika gry rynkowej czy podmiotu zarządzającego kontaktami z osobami fizycznymi niebędącymi pacjentami. Nie wszystkie osoby zatrudnione w podmiocie ochrony zdrowia są wprost związane z wykonywaniem działań polegających na leczeniu osób bądź opieką nad nimi.

W końcu sam podmiot jest nie tylko zakładem pracy, ale też po prostu instytucją wymagającą zwykłego zarządu. Z tą rolą związane jest przetwarzanie danych osobowych zupełnie niedotyczących procesu leczenia. Poza wyżej wymienionymi przepisami pojawiają się osobne zestawy zagadnień prawnych związanych z prawem pracy, tzw. przepisami kadrowymi oraz przepisami dotyczącymi choćby bezpieczeństwa osób i mienia. Niektóre z podmiotów działających w systemie ochrony zdrowia będą jednocześnie instytucjami naukowymi bądź szkołami wyższymi. Ta sama osoba może więc w ramach jednego podmiotu zaangażowanego w system ochrony zdrowia występować jako reprezentant administratora – lub administratorów – w sumie bardzo różnych od siebie. Osoba zatrudniona na uniwersytecie medycznym będzie jednocześnie lekarzem leczącym pacjenta, naukowcem prowadzącym badania naukowe, dydaktykiem prowadzącym zajęcia ze studentami, a przy okazji być może członkiem władz uczelni – dziekanem, rektorem, kierownikiem instytutu czy katedry – lub podmiotem wykonującym działania na rzecz administratorów zewnętrznych. Tak będzie się działo na przykład w przypadku prowadzenia badań klinicznych na rzecz zewnętrznego sponsora. Możemy mieć również do czynienia z różnymi innymi sposobami współpracy z podmiotami zewnętrznymi, na przykład w trakcie testów urządzeń medycznych, oprogramowania czy procedur medycznych.

Jedną z podstawowych zasad, o której musi pamiętać każdy pracujący w tak skomplikowanym środowisku organizacyjnym i prawnym, jest to, że **poszczególnych ról administratora danych osobowych nie można ze sobą „mieszać"**. To, że pracownik szpitala jest jednocześnie jego pacjentem, nie uprawnia administratora danych, jakim jest szpital, do mieszania swoich ról administratora w obu tych zakresach. Z orzeczenia ETPC z 17.7.2008 r. w sprawie I przeciwko Finlandii (skarga Nr 20511/03, Legalis) wynika wyraźnie, że szpital nie może wykorzystywać danych pacjentki, która jest jednocześnie pracownicą szpitala, do kwestii kadrowych, nie mając do tego wyraźnej podstawy prawnej. Sam fakt, że jest w posiadaniu obu tych zestawów informacyjnych – zestawu używanego na potrzeby pracownicze obejmującego przecież również pewne informacje o stanie zdrowia i zasobu przechowywanego jako dane pacjenta – nie oznacza, że można z nich wyciągać wspólne wnioski, a w szczególności podejmować jakiekolwiek działania (przetwarzanie danych na potrzeby w stosunku pracy), korzystając samodzielnie z przejętych danych medycznych pacjentów.

W dzisiejszym interoperacyjnym środowisku systemów informacyjnych taki podział nie jest oczywisty Jednak zadaniem i obowiązkiem administratora danych jest wprowadzenie organizacyjnych zasad, które uniemożliwią takie przetwarzanie danych osobowych, by cele przetwarzania nie uległy pomieszczeniu.

Samo pojęcie danych osobowych występujące w RODO ma dość szeroki zakres. Nie jest to żadne *novum*, jako że z podobnym rozwiązaniem mieliśmy do czynienia nie tylko w dyrektywie 95/46/WE, ale już w Konwencji 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych sporządzonej w Strasburgu 28.1.1981 r. (Dz.U. z 2003 r. Nr 3, poz. 25). „Dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Za możliwą do zidentyfikowania osobę fizyczną uważa się osobę, 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.

Zdając sobie sprawę z możliwości identyfikowania osoby na podstawie danych zawartych w różnych zbiorach medycznych lub gromadzonych przez dłuższy czas, należy podkreślić, że **teoretycznie poprawnie przeprowadzona operacja anonimizacji danych o stanie zdrowia prowadzić powinna do wyłączenia tych danych spod reżimu RODO**. Niemniej rzeczywista anonimizacja w przypadku danych medycznych jest z założenia procesem trudnym. Im bardziej kompletne są dane i im więcej ich jest, tym trudniej doprowadzić do ich całkowitej anonimizacji. Proste usunięcie podstawowych danych identyfikacyjnych nie musi wcale prowadzić do utraty przez dane cech opisanych w definicji danych osobowych. Jest to szczególnie oczywiste w przypadku tzw. chorób rzadkich. Jednocześnie nikomu nie trzeba tłumaczyć, że dla wykonania wielu z badań medycznych prowadzonych do celów naukowych lub w celu tworzenia przyszłych rozwiązań informatycznych wykorzystanie jak największej ilości danych medycznych jest nie tylko przydatne, ale może być wręcz niezbędne.

Klasycznym przykładem operacji, do której mogą być wykorzystane ogromne zasoby danych będących danymi osobowymi poddanych procesowi anonimizacji i tym samym wyłączonych spod reżimu RODO, jest uczenie podmiotu sztucznie inteligentnego (w praktyce systemu informacyjnego) posługującego się rozwiązaniami sztucznej inteligencji na potrzeby jego przyszłego działania. Takie maszynowe uczenie powinno być wykonywane na jak najszerszej bazie przykładowych danych medycznych. Tylko w ten sposób maszyna może nauczyć się, jak wygląda zewnętrzny świat. Jeśli więc przeprowadzamy badanie okulistyczne, które na podstawie zaobserwowanych zmian w oku rodzica mogą określić prawdopodobieństwo wystąpienia u dziecka choroby Recklinghausena, chcielibyśmy skorzystać z jak największej liczby danych wcześniej przebadanych osób wraz z ocenami dokonanymi przez lekarzy specjalistów. Na te potrzeby wykorzystywać będziemy dane, które były danymi osobowymi, ale które odizolowane zostały od danych identyfikujących. „Nauczyciela" prowadzącego zajęcia dla inteligentnej maszyny naprawdę nie interesuje, czy przetwarzane dane pochodzą od osoby X czy od osoby Y. Nie ma to również żadnego znaczenia dla samej maszyny (systemu informacyjnego). Jeżeli przyszła praca ma polegać tylko na ocenie wyniku badania medycznego, maszyna uczyć się będzie jedynie, kiedy lekarz uznał, że zmiana w oku istnieje, a kiedy nie. Na podstawie takiej rozbudowanej bazy, pochodzącej od wielu lekarzy, inteligentna maszyna może w przyszłości pomóc we wstępnej ocenie występowania zmian, wskazujących na podatność na chorobę Recklinghausena.

Jednocześnie wiele innych operacji, które na pierwszy rzut oka wydają się prowadzić do zanonimizowania zapisu medycznego, niekoniecznie prowadzić będzie do takiego efektu. Często przyjmuje się, że użycie w algorytmie deidentyfikującym jednokierunkowej funkcji skrótu spowoduje automatycznie stworzenie anonimowego rekordu, który będzie mógł być uzupełniany kolejnymi zestawami danych, w których dane identyfikacyjne poddano „haszowaniu" przy pomocy tej samej jednokierunkowej funkcji skrótu. W końcu z liczby kontrolnej, która jest wynikiem takiej operacji, nie jesteśmy w stanie odczytać pierwotnych danych identyfikacyjnych. Oczywiście nie mamy tu do czynienia z anonimizacją, a jedynie z pseudonimizacją w rozumieniu RODO, czyli z przetworzeniem danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, któ-

rej dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Dane identyfikacyjne zastąpione zostały jedynie pseudonimem indywidualizującym zapis i *de facto* umożliwiającym połączenie ich z innymi zestawami danych tego samego – choćby nieznanego z imienia i nazwiska – człowieka. Co więcej, systematyczne gromadzenie dalszych zestawów danych o tej samej osobie, dla których dane identyfikacyjne poddano takiemu samemu „haszowaniu", zwiększa prawdopodobieństwo ponownej identyfikacji osoby.

Dane osobowe wykorzystywane w ochronie zdrowia będą miały zawsze charakter kontekstowy. Zawsze muszą być oceniane z wzięciem pod uwagę środowiska, w jakim są przetwarzane, obejmującego cechy pacjenta i innych osób fizycznych (np. rodziny), jak i podmiotu przetwarzającego dane oraz współpracujących z nim innych podmiotów. Dane, o których mówimy, mogą pochodzić od pacjenta – dostarczone przez niego świadomie (np. dane z wywiadu), jak i zaobserwowane u pacjenta przez lekarza lub urządzenie. W tym drugim przypadku pojawia się kilka kolejnych pytań. Choćby pytanie o to, co oznacza pojęcie „danych dostarczonych przez osoby fizyczne". Czy obejmuje ono również te dane, których osoba nie przekazała świadomie?

Zdając sobie sprawę z tego, że wszystkie te pytania stanowią jedynie czubek góry lodowej, który dotąd zaobserwowaliśmy, zachęcam Państwa do zapoznania się z całością dzieła przygotowanego pod redakcją *Dominiki Tykwińskiej-Rutkowskiej* i *Anety Sieradzkiej*.

Listopad 2018 r.

Wojciech Rafał Wiewiórowski