Badania kliniczne w świetle RODO

Natalia Kalinowska[1]
Bartłomiej Oręziak[2]
Marek Świerczyński[3]

Stosowane w praktyce modele ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych w badaniach klinicznych budzą wiele wątpliwości prawnych. Kwestia ta wymaga wyjaśnienia w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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[4]. W niniejszej publikacji autorzy podejmują próbę uzasadnienia interpretacji przepisów RODO ułatwiającej prowadzenie badań klinicznych w Polsce[5]. Zwracają przy tym uwagę na problematykę profilowania uczestników badań klinicznych oraz badaczy i innych członków zespołu badawczego, ponieważ jest to jedno z zagadnień budzących obecnie najwięcej problemów praktycznych.

Uwagi wstępne

Mimo że w rozporządzeniu Parlamentu Europejskiego i Rady (UE) Nr 536/2014 z 16.4.2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE[6] nie określono szczegółowych zasad przetwarzania danych osobowych uczestników badań, to w art. 93 wskazano, że do przetwarzania danych osobowych, które odbywa się na podstawie tego rozporządzenia, stosuje się przepisy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[7]. Natomiast zgodnie z art. 94 RODO, wszelkie odesłania do uchylonej dyrektywy należy traktować jako odesłania do RODO. Oznacza to, że przetwarzanie danych osobowych na podstawie rozporządzenia 536/2014 powinno w pełni odpowiadać wymogom wskazanym w RODO. Na tle art. 94 ust. 2 zd. 1 RODO pojawia się natomiast wątpliwość, jak traktować odesłania nie do całej treści dyrektywy 95/46/WE, lecz do poszczególnych jej przepisów[8]. W doktrynie niemieckiej[9] zaproponowane zostały dwie możliwości wykładni:

– przyjęcie, że takie odesłania należy uznawać za nieistniejące, albo
– poszukiwanie przepisu RODO, który reguluje to samo zagadnienie co wskazany w odesłaniu przepis dyrektywy 95/46/WE.

W naszej ocenie należy podzielić ten drugi pogląd. W świetle art. 93 rozporządzenia UE o badaniach klinicznych należy zauważyć, że nowe przepisy mają wzmacniać prawa osób, których dane dotyczą. Prawa te obejmują prawo dostępu do danych, do ich poprawiania i wycofywania. W rozporządzeniu podkreślono jednak, że pewne ograniczenie tych praw jest niezbędne. Konieczne jest bowiem zapewnienie równowagi pomiędzy wiarygodnością danych z badań klinicznych wykorzystywanych do celów naukowych, jak też bezpieczeństwem uczestników badań klinicznych. Jednym z kluczowych rozwiązań przyjętych w ww. rozporządzeniu jest zastrzeżenie, że wycofanie świadomej zgody nie może mieć wpływu na wyniki przeprowadzonych już działań, takich jak przechowywanie i wykorzystywanie danych uzyskanych na podstawie świadomej zgody przed wycofaniem. Stosowanie RODO w badaniach klinicznych wymaga więc uwzględnienia powyższej zasady zachowania równowagi pomiędzy wiarygodnością danych

[1] Autorka jest doktorantką w Katedrze Prawa Cywilnego i Prawa Prywatnego Międzynarodowego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

[2] Autor jest doktorantem w Katedrze Ochrony Praw Człowieka i Prawa Międzynarodowego Humanitarnego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

[3] Autor jest profesorem w Katedrze Prawa Cywilnego i Prawa Prywatnego Międzynarodowego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

[4] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

[5] Problemy ze stosowaniem przepisów o danych osobowych do badań klinicznych były wielokrotnie podnoszone w doktrynie, zob. m.in.: *K. Forysiak*, *P. Zięcik*, [w:] *T. Brodniewicz* (red.), Badania kliniczne, Warszawa 2015, s. 300–302; *R. Stankiewicz*, [w:] *R. Stankiewicz* (red.), Instytucje rynku farmaceutycznego, s. 99. Nie ulega wątpliwości, że archaiczna i często błędnie stosowana regulacja o ochronie danych osobowych w badaniach klinicznych stanowiła jedną z istotnych barier dla rozwoju badań klinicznych w Polsce. Mowa tutaj o przepisach ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm. – częściowo uchylona; dalej jako: ustawa z 1997 r.), rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 29.4.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 11.12.2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 229, poz. 1536), a także innych ustawach szczególnych zawierających postanowienia odnoszące się do zasad przetwarzania danych osobowych (np. ustawa z 6.11.2008 r. o prawach pacjenta i Rzecznik Praw Pacjenta, t.j. Dz.U. z 2017 r. poz. 1318 ze zm.).

[6] Dz.Urz. UE. L Nr 158, s. 1; dalej jako: rozporządzenie UE o badaniach klinicznych lub rozporządzenie Nr 536/2014.

[7] Dz.Urz. UE L Nr 281, s. 31; dalej jako: dyrektywa 95/46/WE.

[8] *W. Chomiczewski*, [w:] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, s. 1125.

[9] *C. Pilz*, [w:] DS-GVO. Datenschutz-Grundverordnung VO (EU) 2016/679. Kommentar, C.H. Beck 2017, s. 802, za: *W. Chomiczewski*, [w:] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie…, s. 1125.

z badań klinicznych wykorzystywanych do celów naukowych, jak również bezpieczeństwem uczestników badań klinicznych.

Przetwarzanie danych osobowych uczestników badań klinicznych

Podstawą prawną legitymizującą udział w badaniu klinicznym jest świadoma zgoda, o której mowa w art. 29 rozporządzenia UE o badaniach klinicznych. Istnieją natomiast wątpliwości co do określenia właściwej podstawy prawnej przetwarzania danych osobowych (wrażliwych) uczestników takiego badania. Do tej pory powszechnie stosowaną praktyką było uzyskiwanie pisemnej zgody uczestników badań na przetwarzanie ich danych osobowych, czyli stosowanie art. 27 ust. 2 pkt 1 ustawy z 1997 r. o ochronie danych osobowych.

Wydaje się jednak, że w świetle przepisów RODO nie jest konieczne uzyskiwanie odrębnej zgody na przetwarzanie danych wrażliwych uczestników badań. Rozporządzenie to określa bowiem inne (bardziej odpowiednie w porównaniu do zgody) podstawy przetwarzania danych dotyczących zdrowia, które mogą znaleźć zastosowanie w przypadku badań klinicznych. W naszej ocenie kluczowa jest podstawa wskazana w art. 9 ust. 2 lit. j) RODO legitymizująca przetwarzanie szczególnych kategorii danych osobowych, które jest niezbędne do prowadzenia badań naukowych. Jak wskazano w motywie 53 RODO, przetwarzanie danych osobowych do celów naukowych powinno też być zgodne z innymi odpowiednimi przepisami, takimi jak przepisy o próbach klinicznych (tłumaczenie prawidłowe: badań klinicznych), co jednoznacznie wskazuje, że cele naukowe mogą obejmować także badania kliniczne. Dodatkowe potwierdzenie takiego podejścia można odnaleźć w motywie 157 RODO wskazującym, że „przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko, obejmując tym pojęciem na przykład (…), badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych [oraz] badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego". Takie stwierdzenie nie tylko przesądza o dopuszczalności wskazania przesłanki niezbędności przetwarzania danych osobowych do celów badań naukowych, ale także sugeruje, że niezależnie od charakteru tych badań, komercyjnego czy niekomercyjnego, a nawet nieinterwencyjnego zastosowanie będą miały do nich przepisy RODO.

Otwarte pozostaje jednak pytanie o podstawę prawną przetwarzania (zwykłych) danych osobowych uczestników badań klinicznych. W naszej ocenie podstawą legalizującą będzie zgoda uczestnika badania z art. 6 ust. 1 lit. a) RODO. Z uwagi jednak na szczególny charakter tej przesłanki[10], związany z zaostrzeniem wymagań dla zgody[11], administrator musi zadbać, aby zgoda spełniała wymóg „poinformowanej zgody" (*informed consent*)[12], ponieważ tylko w takim przypadku możliwe jest uznanie, że osoba, której dane dotyczą, ma świadomość konsekwencji związanych z wyrażeniem zgody.

W RODO uregulowano nie tylko kwestię wyrażenia zgody, ale także jej wycofania, wskazując, że musi ono być równie łatwe jak jej wyrażenie. Nie określono formy, w jakiej powinno nastąpić wycofanie zgody, jednakże ze względu na wymóg rozliczalności powinna być to forma możliwa do utrwalenia, np. pisemna, elektroniczna, ustna (pod warunkiem jej utrwalenia). Jeżeli więc uczestnik badania złożył ustne oświadczenie o wycofaniu się z badania i cofnięciu zgody na przetwarzanie jego danych osobowych w celu umożliwienia mu uczestnictwa w badaniu, należy tę okoliczność odnotować w CRF (dokumentacji badania klinicznego). Pojawia się tu pytanie o zakres, w jakim nastąpiło wycofanie zgody. Osoba, której dane dotyczą, może wyrazić zgodę w jednym lub w większej liczbie celów, ale także kilka niezależnych zgód. Dlatego każdorazowo administrator powinien zadbać o to, aby był w stanie określić, której ze zgód dotyczyło wycofanie. Uczestnik badania klinicznego może udzielać trzech zgód[13]:

- zgody na przetwarzanie danych (zwykłych) w celu umożliwienia mu uczestnictwa w badaniu;
- zgody na przetwarzanie danych w celu umożliwienia przeprowadzania badań diagnostycznych po wycofaniu się z badania;
- zgody na przetwarzanie danych w celu umożliwienia kontaktów z lekarzem prowadzącym badanie po wycofaniu się z badania.

W powyższej sytuacji cofnięcie każdej z tych zgód należy rozpatrywać niezależnie i podmiot danych powinien mieć wiedzę o możliwości niezależnego wycofania każdej ze zgód[14].

[10] RODO wskazuje na kilka wymogów dot. wyrażenia zgody, które są określone w art. 4 pkt 11 i w art. 7 oraz w motywie 32, 33, 42 i 43. Uwagę należy również zwrócić na wytyczne grupy roboczej art. 29 (wciąż w konsultacjach).

[11] *P. Voigt*, *A. von dem Bussche*, The EU General Data Protection Regulation (GDPR). A Practical Guide, Springer 2017, s. 93.

[12] Wymogi dla poinformowanej zgody zostały określone w wytycznych Grupy Roboczej art. 29 dot. zgody (WP 259). Zgodnie z nimi osoba, której dane dotyczą, powinna co najmniej mieć wiedzę o: (i) tożsamości administratora, (ii) celu każdej operacji przetwarzania, dla których zgoda jest wyrażana, (iii) danych lub kategoriach danych, które będą gromadzone i wykorzystywane, (iv) prawie do wycofania zgody, (v) informacji o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu na podstawie przetwarzanych danych, zgodnie z art. 22 ust. 2, oraz (vi) jeżeli ma to zastosowanie, transferze danych, w tym o możliwym ryzyku przekazywania danych do państw trzecich w przypadku braku decyzji w sprawie odpowiedniego stopnia ochrony i odpowiednich zabezpieczeń.

[13] Uczestnik może udzielać także innych zgód, ale powyższe są zgodami na przetwarzanie danych osobowych i będą podlegały przepisom RODO.

[14] Problematyczna wydaje się kwestia potencjalnego wyrażenia zgody na przetwarzanie danych dotyczących przeżywalności uzyskiwanych z rejestrów prowadzonych przez organy administracji publicznej po wycofaniu się z badania lub zaprzestaniu uczestnictwa w badaniu. Z uwagi na to, że RODO nie chroni danych osobowych osób zmarłych, taka zgoda w naszej ocenie nie powinna być pozyskiwana, chociaż z uwagi na zasadę transparentności za dobrą praktykę należy uznać poinformowanie uczestnika badań o przetwarzaniu jego danych osobowych także w tym celu. W naszej ocenie nie jest konieczne precyzyjne wskazywanie konkretnych rejestrów i baz danych, z których pozyskiwane będą te informacje, ale należy wskazać źródło pozyskiwania danych przez odwołanie się do ich kategorii (np. rejestry prowadzone przez NFZ, MZ, ZUS).

Rozporządzenie UE o badaniach klinicznych stawia wiele wymagań warunkujących ich przeprowadzenie. Jednym z nich jest przedstawienie rozbudowanego formularza świadomej zgody na udział w badaniu przekazywanego pacjentowi przez badacza[15]. Niemniej jednak wykorzystanie tego formularza nie powinno zwalniać badacza od spełnienia obowiązku informacyjnego wymaganego przepisami RODO. Należy zauważyć, że zakres informacji przekazywanych uczestnikowi badania w formularzu świadomej zgody i w ramach obowiązku informacyjnego nie są tożsame. W naszej ocenie rodzi to konieczność uzupełnienia formularza o te informacje, które są wymagane przez art. 13 RODO.

Administrator danych osobowych uczestników badań klinicznych

Właściwe określenie ról pełnionych przez sponsora i badacza w świetle przepisów o ochronie danych osobowych jest bardzo istotne[16]. Uczestnika należy bowiem poinformować m.in. o tym, kto jest administratorem jego danych (nie wykluczamy przy tym możliwości przyjęcia liberalnej interpretacji polegającej na tym, że wystarczające jest wyjaśnienie, kto jest sponsorem badania, uznając domyślnie, że to właśnie on jest administratorem danych), jak również o odbiorcach jego danych osobowych.

Zgodnie z RODO podmioty przetwarzające dane osobowe występują przeważnie w dwóch rolach: administratora danych lub podmiotu, któremu powierzono przetwarzanie danych osobowych (tzw. procesor). Rozporządzenie dopuszcza także możliwość istnienia strony trzeciej, tj. osoby fizycznej, osoby prawnej, organu publicznego lub jednostki, lub podmiotu innego niż:

- osoba, której dane dotyczą;
- administrator;
- podmiot przetwarzający;
- osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe.

Powyższe rozróżnienie ma podstawowe znaczenie dla wyznaczenia zakresu obowiązków określonych w przepisach chroniących dane osobowe, które powinien spełnić administrator, ponieważ głównym adresatem obowiązków określonych w RODO, a także decyzji wydawanych przez organ nadzorczy (Prezesa Urzędu Ochrony Danych Osobowych) jest administrator danych.

Przetwarzanie danych osobowych przez podmiot przetwarzający opiera się na umowie lub innym instrumencie prawnym, a jego odpowiedzialność jest ograniczona treścią tej umowy lub instrumentu prawnego[17]. Odpowiedzialność podmiotu przetwarzającego jest więc znacznie węższa niż odpowiedzialność spoczywająca na administratorze danych[18].

Próba określenia zakresu odpowiedzialności strony trzeciej jest natomiast bezcelowa, ponieważ RODO poza zdefiniowaniem zakresu podmiotowego tego pojęcia nie wymienia jej praw i obowiązków. Jedynie art. 6 ust. 2 lit. f) RODO wskazuje na możliwość istnienia prawnie uzasadnionych interesów realizowanych przez tę stronę trzecią, ale nawet w tym zakresie poinformowanie o tych interesach, a także o tym, że strona trzecia jest odbiorcą danych osobowych, spoczywa na administratorze danych.

W rozporządzeniu ogólnym zawarta jest także definicja legalna administratora danych (art. 4 pkt 7 RODO). Jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W praktyce administratorem danych jest podmiot, który samodzielnie lub wspólnie z innym podmiotem, bądź za pomocą innych podmiotów, przetwarza dane osobowe na własne potrzeby.

Odpowiadając na pytanie o rolę sponsora, badacza i ośrodka badawczego w świetle przepisów RODO, należy rozważyć co najmniej trzy modele ochrony danych:

1) sponsor, badacz i ośrodek są współadministratorami danych osobowych;
2) sponsor jest administratorem danych, a badacz i ośrodek badawczy są podmiotami przetwarzającymi (procesorami);
3) sponsor jest stroną trzecią, badacz administratorem danych, a ośrodek badawczy procesorem.

1. Sponsor, badacz i ośrodek jako współadministratorzy danych osobowych

Zgodnie z RODO, jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami (art. 26 RODO). Z podanej definicji wynika, że aby mówić o współadministratorach, muszą być spełnione równocześnie trzy warunki:

1) podmiot lub podmioty muszą być administratorami danych osobowych w rozumieniu RODO;
2) muszą wspólnie ustalić cele przetwarzania danych;
3) muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych[19].

[15] *M. Krasińska*, [w:] *M. Jagielski*, *M. Krasińska*, *P. Kawczyński*, *K. Wojsyk*, *A. Sieradzka*, *E. Bielak-Jomaa*, *K. Andres*, Ochrona danych osobowych medycznych, Warszawa 2016, s. 41 i n.

[16] Na temat ochrony danych osobowych pacjenta – uczestnika badania w prawie wspólnotowym i francuskim zob. *I. de Lamberterie*, *H.J. Lucas*, Informatique, libertés et recherche médicale, Paris 2001.

[17] Szerzej na ten temat: *B. Van Alsenoy*, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, Journal of Intellectual Property, Information Technology and E-Commerce Law 2016, Nr 3, https://www.jipitec.eu/issues/jipitec-7-3-2016/4506 (dostęp 21.4.2018 r.).

[18] *P. Litwiński*, [w:] *M. Jagielski*, *M. Krasińska*, *P. Kawczyński*, *K. Wojsyk*, *A. Sieradzka*, *E. Bielak-Jomaa*, *K. Andres*, Ochrona danych…, s. 47 i n.

[19] *A. Buczyńska-Borowy*, Współadministratorzy i proces współadministrowania, ABI Expert 2017, Nr 2, s. 44.

W RODO nie wskazuje się, co oznacza wspólne ustalanie takich celów. Nie jest jasne, czy stosunek współadministrowania będzie zachodził także wtedy, gdy dany podmiot, realizując proces przetwarzania, samodzielnie określi cele lub sposoby przetwarzania, na które zgodzą się pozostałe podmioty. W tym zakresie wypowiedziała się jednak Grupa Robocza[20], która w swojej opinii z 2010 r. wskazała, że sam fakt, że w procesie przetwarzania danych osobowych współpracują różne podmioty, np. w łańcuchu, nie oznacza, że są one wspólnymi administratorami we wszystkich przypadkach, ponieważ wymianę danych między dwiema stronami przy braku wspólnych celów lub sposobów przetwarzania w ramach wspólnej grupy operacji należy uważać wyłącznie za przekazywanie danych pomiędzy dwoma oddzielnymi administratorami danych. Trzeba zawsze badać skalę mikro i makro przetwarzania, ponieważ możliwe jest, że w skali mikro poszczególne operacje przetwarzania danych w łańcuchu wydają się niepowiązane, jako że każda z nich może mieć inny cel, ale już w skali makro możliwe byłoby uznanie operacji przetwarzania danych za „grupę operacji" służących jednemu celowi lub wykorzystujących wspólnie określone sposoby przetwarzania danych.

Przyjmując więc, że poszczególne cele przetwarzania danych osobowych w procesie w skali mikro realizowane przez sponsora, badacza i ośrodek badawczy, służą wspólnemu celowi całego procesu (w skali makro), w naszej ocenie możliwe jest przyjęcie, że między tymi podmiotami będzie zachodził stosunek współadministrowania. Ponadto uważamy, że każdy z celów realizowanych w skali mikro powinien być niezbędny do realizacji celu w skali makro oraz powinien być znany pozostałym współadministratorom.

2. Sponsor jest administratorem danych, a badacz i ośrodek badawczy są procesorami

Jeżeli natomiast przyjąć literalne brzmienie przepisu, które zakłada, że cele i sposoby przetwarzania muszą być ustalane wspólnie, należy uznać sponsora za administratora danych osobowych. Z kolei badacz i ośrodek badawczy będą podmiotami, które przetwarzają dane osobowe w imieniu administratora (art. 4 pkt 8 RODO). Należy zauważyć, że jest to pogląd dominujący, choć z uwagi na charakter danych, do których ma dostęp sponsor, może budzić wątpliwości. Za uznaniem go za administratora danych przemawia jednak, że to on zleca i finansuje badania, a także zapewnia udział w badaniu przez pracownika lub przedstawiciela firmy sponsorującej badania kliniczne (tzw. monitora, tj. osoby monitorującej badania) i audytora. Posiada więc uprawnienia o charakterze nadzorczym. Celem uporządkowania rozważań w dalszej części opracowania będziemy jednak, mówiąc o administratorze danych, odnosić się do sponsora.

3. Sponsor jest stroną trzecią, badacz administratorem a ośrodek badawczy procesorem

Za problematyczną z perspektywy oceny roli sponsora należy uznać zasadę, zgodnie z którą dane pacjentów są pozbawione funkcji identyfikacyjnej dla sponsora[21] po dokonaniu pseudonimizacji lub anonimizacji danych pacjentów. Pseudonimizacja skutkuje niemożliwością przypisania informacji do konkretnej osoby, której dane dotyczą, bez użycia dodatkowych informacji, przy czym takie dodatkowe informacje są przechowywane osobno objętymi środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (w dokumentacji badania prowadzonej przez badacza). Informacje te nadal jednak stanowią dane osobowe w rozumieniu RODO. Natomiast po dokonaniu anonimizacji nie ma już możliwości, nawet przy użyciu dodatkowych informacji, zidentyfikowania poszczególnych uczestników badania. W takim układzie sponsor pozbawiony narzędzia pozwalającego na ponowną identyfikację uczestników badania w ogóle nie przetwarza danych osobowych[22] i w związku z powyższym nie jest możliwe wykonywanie przez niego praw osób, których dane dotyczą, np. prawa dostępu do danych czy prawa do przenoszenia[23]. W takim przypadku zasadne byłoby rozważenie uznanie sponsora za stronę trzecią, która ma interes w przeprowadzaniu takich badań, ale nie w dostępie do danych osobowych. Dane osobowe są przetwarzane przede wszystkim przez badacza, który prowadzi badania kliniczne i ma faktyczny wpływ na cele i sposoby ich przetwarzania, mając jednocześnie bezpośredni kontakt z uczestnikiem badań (mimo że to sponsor zleca i finansuje badania kliniczne). Natomiast ośrodek badawczy stanowi miejsce, w którym badanie ma być przeprowadzone, i w ograniczonym zakresie może przetwarzać dane osobowe uczestników badań w celu określonym przez administratora danych. Mimo powyższych argumentów uważamy, że model ten budzi najwięcej wątpliwości prawnych.

[20] Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", s. 20–24.

[21] *W. Wiewiórowski*, Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych, Europejski Przegląd Sądowy 2017, Nr 5, s. 28.

[22] Zgodnie z definicją z art. 4 pkt 7 RODO „administrator oznacza osobę (…) [która] samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych". Skoro sponsor nie przetwarza danych osobowych, to nie spełnia wszystkich przesłanek z definicji pozwalających uznać go za administratora.

[23] *W. Wiewiórowski*, Prawo do przenoszenia…, s. 28.

Wymogi przetwarzania danych osobowych w badaniach klinicznych

RODO nakłada na podmioty przetwarzające dane osobowe wiele obowiązków. W kontekście badań klinicznych w szczególności jest istotne zachowanie zgodności z regułą minimalizacji przetwarzanych informacji (zapewnienie, że dane osobowe są przetwarzane jedynie w niezbędnym zakresie, nie dłużej niż przez czas wymagany do osiągnięcia celów, w związku z którymi są przetwarzane), regułą poufności informacji przetwarzanych (zapewnienie, że dane osobowe są udostępniane jedynie osobom upoważnionym i zabezpieczone przed dostępem osób nieupoważnionych[24]), regułą rozliczalności (bazującą na prawnej odpowiedzialności za właściwe wypełnianie obowiązków wynikających z rozporządzenia[25] i nakładającą na administratora obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać) oraz regułą integralności przetwarzanych informacji (zapewnienie dokładności i kompletności danych osobowych, nienaruszalności danych, tj. ochrona przed nieuprawnionym ich zmienianiem bądź zniszczeniem). Szczególnie istotne jest uwzględnienie tych zasad w przypadku badań klinicznych, które są prowadzone w interesie publicznym. Jak wynika z RODO, przetwarzanie w tym celu odbywa się w zgodzie z przepisami prawa Unii lub prawa państwa członkowskiego, które powinno zapewnić odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową. Rodzi to pytanie o zasadność wykorzystania tej przesłanki, w przypadku gdy przepisy nie zapewniają takiej ochrony. Dodatkowym problemem jest trudność dokonania oceny, jakie środki są odpowiednie i konkretne. Nie wydaje się jednak, aby ocena ta miała spoczywać na administratorze danych osobowych.

W RODO zawarto zamknięty katalog przesłanek legalności przetwarzania danych osobowych zwykłych (art. 6) i szczególnych kategorii danych osobowych, zwanych także danymi wrażliwymi czy sensytywnymi (art. 9). Ten ostatni przepis, jako całość, został skonstruowany odmiennie niż art. 6 RODO określający podstawy prawne przetwarzania tzw. danych zwykłych. W art. 9 ust. 1 RODO ustanowiono bowiem generalny zakaz przetwarzania danych osobowych, które mogą być uznane za dane wrażliwe, natomiast ust. 2 tego przepisu określa sytuacje, w których zakaz ten został uchylony[26] (np. prowadzenie badań naukowych, do której to kategorii należą badania kliniczne). Spełnienie którejkolwiek z nich skutkuje dopuszczalnością przetwarzania danych.

W ramach danych osobowych przetwarzanych przy okazji prowadzenia badań klinicznych przetwarzane są przede wszystkim szczególne kategorie danych, a zwłaszcza dane dotyczące zdrowia. Przesłanek legalizujących ich przetwarzanie należy więc szukać w art. 9 RODO. W przypadku badań klinicznych zastosowanie znajdą przede wszystkim dwie przesłanki z art. 9 ust. 2 lit. i oraz j RODO, tj. niezbędność przetwarzania ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego oraz niezbędność przetwarzania do celów badań naukowych.

Oprócz konieczności wykazania podstawy do przetwarzania danych osobowych na administratorze ciążą ponadto liczne obowiązki informacyjne w stosunku do osób, których dane są zbierane. Informacje te powinny zostać przekazane na etapie zbierania danych osobowych. Zakres i sposób przekazywania tych informacji jest określony odpowiednio w art. 12 i n. RODO. Artykuł 13 RODO wskazuje informacje przekazywane przez administratora danych, w przypadku gdy ten pozyskał dane bezpośrednio od podmiotu danych osobowych, natomiast art. 14 RODO odnosi się do pozyskiwania danych z innych źródeł.

W przypadku pozyskiwania danych od podmiotu danych administrator podaje osobie, której dane dotyczą, następujące informacje:

- swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
- gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
- cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Ponadto aby przetwarzanie było rzetelne i przejrzyste dla osoby, której dane dotyczą, administrator podaje:

- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

[24] *P. Barta*, *M. Kawecki*, [w:] *P. Litwiński* (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Legalis/el. 2018.

[25] *P. Drobek*, [w:] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie…, s. 342.

[26] *P. Barta*, *M. Kawecki*, [w:] *P. Litwiński* (red.), Rozporządzenie UE w sprawie ochrony…, Legalis/el. 2018.

– informacje o prawie wniesienia skargi do organu nadzorczego;
– informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Zakres informacji podawanych w przypadku pozyskiwania danych z innych źródeł obejmuje dodatkowo kategorie przetwarzanych o tej osobie danych osobowych oraz informacje o źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

Przetwarzanie danych osobowych badaczy i innych członków zespołu badawczego

Niezależnie od faktu przetwarzania danych osobowych uczestników badania klinicznego należy także rozważyć zagadnienie przetwarzania danych osobowych członków zespołu badawczego. W tym zakresie na podstawie umowy o przeprowadzenie badania klinicznego sponsor jest administratorem danych osobowych badaczy, a przesłanką przetwarzania ich danych jest niezbędność do wykonania tej umowy (art. 6 ust. 1 pkt b RODO). Powstaje pytanie, czy współbadacze oraz inne osoby wchodzące w skład zespołu powinni udzielać zgody na przetwarzanie ich danych osobowych w odrębnym formularzu, w sytuacji gdy sponsor nie zawrze z nimi odrębnych umów. Nie podzielamy opinii, że zgoda powinna stanowić podstawę przetwarzania tych danych. W naszej ocenie znacznie bardziej właściwa byłaby przesłanka prawnie uzasadnionego interesu administratora danych. Zastosowanie tej przesłanki jest możliwe, jeśli nadrzędne wobec tych interesów okazałyby się prawa i wolności tych osób, co w przypadku członków zespołu badawczego nie ma miejsca. Ponadto jak wskazano w motywie 47 RODO, taki prawnie uzasadniony interes może istnieć w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Właśnie taka sytuacja zachodzi w przypadku prowadzenia badań klinicznych, gdyż badacze działają na rzecz sponsora zlecającego te badania. Zgoda na przetwarzanie danych osobowych w powyższym celu nie wydaje się więc ani potrzebna, ani celowa. Zdajemy sobie jednak sprawę, że propozycja ta stanowi istotne *novum*, gdy chodzi o polską praktykę realizacji badań klinicznych.

W tym zakresie wątpliwości może budzić kwestia przetwarzania danych osobowych badaczy i innych członków zespołu badawczego, wykraczających poza zakres tzw. danych służbowych (np. adres prywatny, numer dowodu osobistego), które jednak są wykorzystywane (przetwarzane) w związku z realizacją umowy łączącej sponsora z badaczem (np. prawidłowe dokonanie rozliczeń). Wydaje się, że z uwagi na wskazanie dokonane w motywie 47 RODO podstawą przetwarzania tych danych także będzie prawnie uzasadniony cel administratora danych.

Powierzenie przetwarzania danych osobowych w badaniach klinicznych

W art. 28 RODO określono zasady umownego powierzenia danych osobowych. Dane mogą zostać powierzone na mocy umowy lub innego instrumentu prawnego. Ta umowa lub inny instrument prawny mogą mieć formę pisemną lub elektroniczną. Umowa ta musi określać przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora i podmiotu przetwarzającego. Obowiązki administratora zostały określone w art. 24 RODO. Podmiot przetwarzający pomaga w spełnieniu tych obowiązków oraz wypełnia obowiązki z art. 28 ust. 3 RODO zgodnie z umową, w której wszystkie te obowiązki powinny być określone.

Jeśli uznać, że sponsor jest administratorem danych, to ośrodek badawczy oraz badacza należy uznać za podmioty przetwarzające, które będą przetwarzały dane na udokumentowane polecenie sponsora. Pewne trudności przy tej konstrukcji może rodzić kwestia obowiązku korzystania przez sponsora tylko z takich badaczy i takiego ośrodka badawczego, którzy zapewniają odpowiednie gwarancje spełnienia wymogów wynikających z RODO. W doktrynie wskazuje się, że wybór takiego procesora przez administratora powinien być uważny, a współpraca z podmiotami niedającymi odpowiednich gwarancji jest wykluczona[27].

Procesor odpowiada wyłącznie w zakresie określonym umową powierzenia[28]. W szczególności podejmuje wszelkie środki dotyczące bezpieczeństwa przetwarzania wymagane na mocy art. 32 RODO, przestrzega warunków dotyczących podpowierzenia danych innemu podmiotowi, pomaga sponsorowi wywiązać się z obowiązku odpowiadania na żądania podmiotów danych (uczestników badań) oraz wywiązać się z obowiązków w zakresie bezpieczeństwa przetwarzania zgłaszania naruszeń ochrony danych, zawiadamiania osoby, której dane dotyczą, o takim naruszeniu oraz wspiera administratora w zakresie dokonywania oceny skutków dla ochrony danych, a także w ramach procedury uprzednich konsultacji. Ponadto badacz/ośrodek badawczy występujący

[27] *K. Witkowska-Nowakowska*, [w:] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie…, s. 635.

[28] *P. Litwiński*, [w:] *M. Jagielski*, *M. Krasińska*, *P. Kawczyński*, *K. Wojsyk*, *A. Sieradzka*, *E. Bielak-Jomaa*, *K. Andres*, Ochrona danych…, s. 47 i n.

w roli procesorów powinni udostępniać administratorowi wszelkie informacje niezbędne do wykazania spełnienia jego obowiązków określonych w art. 32 RODO oraz umożliwiać administratorowi danych lub upoważnionemu przez niego audytorowi przeprowadzanie audytów – w naszej ocenie, może to obejmować także umożliwianie udziału w badaniu przez monitora i audytora.

Podstawowym zadaniem podmiotu, któremu powierzono przetwarzanie danych osobowych, jest więc zabezpieczenie ich przetwarzania. W tym zakresie należy zauważyć, że RODO nie przesądza, jakie środki powinny zostać zastosowane przez procesora. Jest to wynikiem podejścia opartego na ryzyku, tj. konstrukcji bazującej na kształtowaniu obowiązków, których zakres określany jest przez pryzmat oceny ryzyka[29]. Wątpliwa jest możliwość realizacji tego wymogu przez badaczy i ośrodki, które nie przeprowadziły stosownego wdrożenia RODO w swoich organizacjach (działalności).

Przez umowy powierzenia przetwarzania danych osobowych należy rozumieć wszelkie umowy, do wykonania których zleceniobiorca przetwarza dane osobowe administratora (bez względu na to, czy przetwarzanie danych stanowi jej istotę, czy też następuje tylko „przy okazji"). Ponadto brak zawarcia takiej umowy między administratorem danych a podmiotem przetwarzającym (niezależnie czy za administratora danych uznajemy sponsora czy badacza) nie powoduje, że do powierzenia danych faktycznie nie dochodzi[30].

Problematyczne wydaje się natomiast określenie, jak należy dokonywać powierzenia przetwarzania danych, w sytuacji gdy założy się, że między sponsorem, badaczem i ośrodkiem badawczym dochodzi do współadministrowania przetwarzanymi danymi osobowymi. Jak wskazuje się w literaturze[31], w takim przypadku każdy ze współadministratorów powinien zawierać umowy powierzenia w zakresie przypisanych mu celów i sposób przetwarzania, chyba że wspólne uzgodnienia w ogóle wyłączały możliwość umownego powierzenia.

Niedopełnienie wymogów z art. 28 RODO wiąże się z ryzykiem nałożenia administracyjnej kary pieniężnej w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Jeśli jednak administrator danych lub podmiot przetwarzający naruszą podstawowe zasady przetwarzania szczególnych kategorii danych osobowych (w tym danych dotyczących zdrowia), to kara pieniężna może wynieść do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Jeśli więc w wyniku prowadzonych badań klinicznych doszłoby do naruszenia obejmującego zarówno niedopełnienie obowiązków określonych w art. 28 RODO, jak i przetwarzanie szczególnych kategorii danych, to z uwagi na to, że do naruszeń doszło w ramach tych samych lub powiązanych operacji przetwarzania danych, kara wyniosłaby maksymalnie do 20 000 000 euro lub do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Jeśli jednak do obu naruszeń doszłoby w ramach niepowiązanych ze sobą badań klinicznych (operacji przetwarzania danych), procesor lub administrator danych odpowiadałby za każde naruszenie z osobna.

Poza odpowiedzialnością pieniężną, w nowej polskiej ustawie z 10.5.2018 r. o ochronie danych osobowych[32], mając na względzie dobro podmiotów danych oraz wagę naruszenia, jakim jest przetwarzanie danych osobowych, uznano, że przetwarzanie danych bez podstawy prawnej, a więc nieuprawnione i umyślne przetwarzanie, powinno być zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności[33]. W zakresie maksymalnej kary (pozbawienia wolności) ustawodawca dokonał rozróżnienia i w zależności od kategorii danych – wskazał ją na poziomie dwóch lat pozbawienia wolności w przypadku naruszenia zasad ochrony danych zwykłych oraz trzech lat pozbawienia wolności w przypadku naruszenia zasad ochrony danych wrażliwych.

Profilowanie w badaniach klinicznych

1. Profilowanie w świetle wytycznych Grupy Roboczej art. 29

Grupa Robocza art. 29[34] w swoich wytycznych dot. profilowania i automatyzowanego podejmowania decyzji[35] wyróżnia profilowanie ogólne, podejmowanie decyzji oparte na profilowaniu oraz wyłącznie zautomatyzowane podejmowanie decyzji oparte na profilowaniu[36].

W ocenie Grupy Roboczej profilowanie składa się z trzech elementów:

1) musi stanowić formę zautomatyzowanego przetwarzania;
2) musi być przeprowadzane na danych osobowych i
3) celem profilowania musi być ocena osobistych aspektów dotyczących osoby fizycznej[37].

[29] *D. Lubasz*, [w:] *E. Bielak-Jomaa* (red.), *D. Lubasz* (red.), RODO. Ogólne rozporządzenie…, s. 692.

[30] *K. Witkowska-Nowakowska*, [w:] *E. Bielak-Jomaa* (red.), *D. Lubasz* (red.), RODO. Ogólne rozporządzenie…, s. 634.

[31] *J. Byrski*, Umowne powierzenie do przetwarzania danych osobowych w ustawie o ochronie danych osobowych, dyrektywie 95/46 i w ogólnym rozporządzeniu o ochronie danych, MoP 2016, Nr 20, s. 39.

[32] Dz.U. poz. 1000 ze zm.

[33] Uzasadnienie do projektu nowej ustawy o ochronie danych osobowych, s. 40–41; https://legislacja.rcl .gov.pl/docs//2/12302950/12457690/12457691/dokument334234.pdf (dostęp z 20.3.2018 r.).

[34] Grupa Robocza Art. 29 została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności.

[35] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251).

[36] *Ibidem*, s. 8.

[37] *Ibidem*, s. 6.

Na bardzo ogólnym poziomie profilowanie wiąże się z kategoryzowaniem osób według ich cech „niezmiennych" (takich jak płeć, wiek, pochodzenie etniczne, wzrost) czy „zmiennych" (takich jak zwyczaje, preferencje i inne elementy zachowania)[38]. Zazwyczaj profile tworzy się za pomocą techniki zwanej „analizą behawioralną". Polega ona na dopasowaniu i korelacji określonego zachowania (np. wyborów konsumenckich) z cechami (np. wiek)[39].

Profilowanie może również wykorzystywać inne dane niż pochodzące i powiązane z podmiotem danych, np. dane statystyczne. Profile tego rodzaju opierają się na prognozowaniu różnych postaw ludzkich na podstawie zestawiania danych wielu osób i następnie określaniu statystycznego prawdopodobieństwa tych zachowań. Do uprzednio przygotowanych modeli „dopasowywane" są więc konkretne osoby. Rodzi to ryzyko przypisania im cech, których w istocie one nie mają, co z kolei prowadzić może do nieusprawiedliwionego pozbawienia ich dostępu do pewnych dóbr i usług[40]. Dlatego często jest wykorzystywane do przewidywania ludzkich zachowań przy użyciu danych z różnych źródeł w celu sformułowania wniosków o danej osobie, na podstawie cech innych osób, które wyglądają statystycznie podobnie[41]. W takim przypadku ryzyko dyskryminacji jest znacznie wyższe.

Opinia Grupy Roboczej art. 29 dotycząca profilowania[42] początkowo była bardzo restrykcyjna – zdaniem Grupy nawet proste ocenianie czy klasyfikacja osób na podstawie cech takie jak wiek, płeć i wzrost mogło być uznane za profilowanie, niezależnie od tego, czy było skorelowane z jakimkolwiek celem predykcyjnym[43]. Rewizja wytycznych[44] przyniosła złagodzenie tego stanowiska. Grupa wskazała, że prosta klasyfikacja osób na podstawie znanych cech, takich jak wiek, płeć i wzrost, niekoniecznie musi prowadzić do profilowania. Zasadniczo będzie to zależeć od celu klasyfikacji[45]. Takie podejście należy ocenić pozytywnie, ponieważ nie wydaje się, aby prosta klasyfikacja, przy której podmiot danych łatwo może ocenić jej zasady, miała być objęta ochroną równoważną ze skomplikowanymi procesami przetwarzania, dokonywanymi z wykorzystaniem np. bardzo dużej ilości zmiennych, algorytmów czy danych o tej osobie, niepochodzących bezpośrednio od niej albo zestawiania jej danych z danymi statystycznymi dla profilu, który powstał w oparciu o dane pochodzące od tej osoby. Z uwagi na to, że ludzie mają różne poziomy zrozumienia złożonej techniki związanej z profilowaniem i automatycznymi procesami decyzyjnymi to działania te mogą być dla nich wyzwaniem[46]. Osoby, których dane są przetwarzane w taki sposób, mogą nie tylko nie rozumieć przyczyn i przebiegu samego procesu przetwarzania, ale wręcz nie mieć wiedzy o tym, że w ogóle się ono odbywa[47].

Należy także podzielić opinię Grupy Roboczej, zgodnie z którą zautomatyzowanym podejmowaniem decyzji obejmującym przetwarzanie nie jest prosta klasyfikacja służąca uzyskaniu zbiorczego przeglądu np. swoich klientów bez dokonywania jakichkolwiek prognoz ani wyciągania wniosków na temat konkretnej osoby. W takim przypadku nie dochodzi do profilowania, ponieważ celem nie jest ocena indywidualnych cech[48].

2. Profilowanie w świetle RODO

Zgodnie z art. 4 pkt 4 RODO profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, przeznaczoną do analizowania lub prognozowania osobowości bądź niektórych czynników osobowych osoby fizycznej, w szczególności analizy i prognozy jej zdrowia, sytuacji ekonomicznej, efektów jej pracy, osobistych preferencji lub zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się[49]. Z tej definicji wynika, że profilowanie nie dotyczy przypadków niezautomatyzowanego (ręcznego) przetwarzania danych.

Wyróżnia się dwa rodzaje profilowania:

1) profilowanie zwykłe,
2) profilowanie kwalifikowane.

[38] Agencja Praw Podstawowych, Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu. http://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_PL.pdf (dostęp z 16.12.2017 r.).

[39] *J. Niklas*, Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji, http://ptpa.org.pl/site/ assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf (dostęp z 16.12.2017 r.).

[40] *X. Konarski*, Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce, MoP 2016, Nr 20, s. 49, za: Rekomendacja CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, s. 2.

[41] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251), s. 7.

[42] *Ibidem*.

[43] *Ibidem*.

[44] *Ibidem*.

[45] *Ibidem*.

[46] Szczególnie zautomatyzowane decyzje podejmowane z wykorzystaniem sztucznej inteligencji (*artificial intelligence*, AI) czy systemów samouczących (*machine learning*, ML) stwarzają ryzyko niezrozumienia motywów podjęcia takiej decyzji i w efekcie zagrażają autonomii informacyjnej. Podobnie w tym zakresie wypowiada się: *M. Hildebrandt*, The Dawn of a Critical Transparency Right for the Profiling Era, https://works.bepress.com/mireille_hildebrandt/40/download/ (dostęp z 21.4.2018 r.); *ML. Jones*, Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood, Soc Stud Sci 2017, Nr 47.

[47] Guidelines on Automated individual…, s. 17.

[48] *Ibidem*, s. 7.

[49] „Profiling" means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements.

Profilowanie zwykłe	Profilowanie kwalifikowane
Art. 4 pkt 4 RODO	Art. 22 RODO
Dowolna forma zautomatyzowanego przetwarzania[50]	Forma wyłącznie zautomatyzowanego przetwarzania[51]
Brak decyzji lub decyzja: – niewywołująca skutków prawnych. – niewpływająca na osobę, której dane dotyczą. – niewpływająca istotnie na osobę, której dane dotyczą	Decyzja wywołująca skutki prawne lub w podobny sposób istotnie wpływająca na osobę, której dane dotyczą

Źródło: *N. Kalinowska* – opracowanie własne.

Rozporządzenie o ochronie danych osobowych wielokrotnie odnosi się do profilowania osoby fizycznej. Słowo profilowanie w samym rozporządzeniu pojawia się 23 razy. Jak wskazano powyżej, przetwarzanie danych osobowych z wykorzystaniem profilowania zwykłego i profilowania kwalifikowanego jest objęte zupełnie innym reżimem ochronnym. Wymagany poziom ochrony jest zależny od ryzyka dla ochrony praw i wolności osób, których dane dotyczą. RODO stanowi, że im ryzyko związane z przetwarzaniem danych osobowych jest większe, tym większy powinien być zakres obowiązków ciążących na administratorze danych[52].

3. Zautomatyzowane podejmowanie decyzji obejmujące profilowanie

Na gruncie RODO wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, istnieje zwłaszcza w tych sytuacjach, gdy profilowanie jest elementem przetwarzania, o którym mowa w art. 22 RODO. Jak wskazuje motyw 71 RODO, do takiego przetwarzania zalicza się „profilowanie", ale tylko wtedy, gdy wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. W doktrynie wskazuje się na trudność z ustaleniem, jakie decyzje można uznać za wpływające na osobę w podobny sposób, jak decyzje o skutkach prawnych[53]. Wskazuje się, że może być decyzja prowadząca do niezawarcia umowy. W takim przypadku nie powstają bowiem skutki prawne, a zatem konieczne jest – w interesie podmiotów danych – posłużenie się dodatkowym kryterium „istotnego wpływu"[54]. Również wytyczne Grupy Roboczej art. 29 wskazują, że aby przetwarzanie danych znacząco wpłynęło na podmiot danych, efekty przetwarzania muszą być wystarczające duże lub ważne, aby być godnym uwagi. Innymi słowy, decyzja musi potencjalnie:

– znacząco wpłynąć na okoliczności, zachowania lub wybory osoby, której dane dotyczą;
– mieć długotrwały lub trwały wpływ na osobę, której dane dotyczą lub
– w najbardziej skrajnym przypadku prowadzić do wykluczenia lub dyskryminacji osób.

Dodatkowo Grupa Robocza uznaje, że wystarczająco istotnym skutkiem są m.in. decyzje wpływające na czyjś dostęp do usług zdrowotnych. Wydaje się więc, że profilowanie wykorzystywane w badaniach klinicznych w rozumieniu RODO może powodować takiego rodzaju istotne skutki dla osoby, której dane dotyczą, ponieważ niemożność wzięcia udziału w badaniu klinicznym pozbawia pacjenta dostępu do leku i terapii z nią związanej, która potencjalnie mogłaby poprawić jego stan zdrowia.

Warto zauważyć, że jeśli zautomatyzowane podejmowanie decyzji, o którym mowa w art. 22 RODO, będzie obejmowało przetwarzanie szczególnych kategorii danych, administrator będzie mógł je zastosować tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na nie wyraźną zgodę lub gdy będzie ono niezbędne ze względów związanych z ważnym interesem publicznym. RODO wymaga, aby poza istnieniem jednej z dwóch przesłanek legalizujących dodatkowo istniały właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, nie wskazując jednak, kto ma je zapewnić. W przypadku przesłanki z art. 9 ust. 2 lit. g) RODO, która mówi o ważnym interesie publicznym wprost wskazano, że w przepisach prawa Unii lub państwa członkowskiego mają być przewidziane odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Wydaje się więc, że przy oparciu przetwarzania danych dotyczących zdrowia w ramach badań klinicznych na przesłance z art. 9 ust. 2 lit. g) RODO administrator nie będzie zobligowany do podejmowania dodatkowych działań na rzecz zapewnienia takich środków ochrony. Taki pogląd jest jednak

[50] W wersji angielskiej rozporządzenie posługuje się wyrażeniem dowolnej/jakiejkolwiek formy (*any form*).

[51] W angielskiej wersji rozporządzenia wprost wskazano, że taka decyzja opiera się wyłącznie (*solely*) na zautomatyzowanym przetwarzaniu.

[52] *M. Byczkowski*, Znaczenie norm ISO we wdrażaniu bezpieczeństwa technicznego i organizacyjnego wymaganego w RODO, MoP 2017, Nr 20, s. 17.

[53] *S. Wachter*, *B. Mittelstadt*, *L. Floridi*, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law 2017, Nr 2, s. 93.

[54] *X. Konarski*, Profilowanie danych osobowych…, s. 50.

możliwy do zaakceptowania jedynie w przypadku uznania, że pojęcie „właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą" jest tożsame z pojęciem „odpowiednich i konkretnych środków ochrony praw podstawowych i interesów osoby, której dane dotyczą". Odnosząc się do art. 22 ust. 3 RODO, można uznać, że właściwe środki ochrony obejmują co najmniej prawo do uzyskania interwencji ludzkiej ze strony administratora do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Jeśli więc przepisy prawa będą gwarantować przynajmniej taki zakres ochrony, to należy uznać, że podejmowanie dodatkowych działań przez administratora nie jest wymagane.

Z drugiej strony, w kontekście przeprowadzania badań klinicznych należy mieć na uwadze treść motywu 71 RODO, zgodnie z którym administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające, w szczególności korektę powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą. Ma to na celu ograniczenie negatywnych skutków:

1) w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną lub
2) skutkujący środkami mającymi taki efekt.

Mimo że zalecenie to wynika z motywu, w naszej ocenie, z uwagi na kontekst przetwarzania danych uczestników badań klinicznych jednym z działań, które powinny zostać podjęte przez administratora, jest wdrożenie i stosowanie takich procedur i środków. Aby zapewnić należytą ochronę szczególnym kategoriom danych osobowych zautomatyzowane podejmowanie decyzji i profilowanie na nich oparte powinno być dozwolone wyłącznie przy zachowaniu powyżej opisanych warunków.

Profilowanie skutkujące zautomatyzowanym podejmowaniem decyzji zawiera w sobie zarówno element tzw. prawa pozytywnego, jak i negatywnego. Osoba, której dane dotyczą, ma bowiem prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu jej danych, których skutkiem jest podjęcie decyzji o skutku prawnym lub podobnie istotnym (prawo negatywne), ale ma również prawo do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji (prawo pozytywne), co jest przejawem woli ustawodawcy unijnego, aby osoby, których dane dotyczą, miały wiedzę o takim przetwarzaniu i aby było ono dla nich transparentne[55].

Warto w tym miejscu przypomnieć, że rozporządzenie UE w sprawie badań klinicznych produktów leczniczych wprowadza definicję legalną badań klinicznych. Zgodnie z jej treścią „badanie kliniczne" oznacza badanie biomedyczne[56] spełniające którykolwiek z następujących warunków:

a) przydział uczestnika do danej strategii terapeutycznej ustalany jest z góry i odbywa się w sposób niestanowiący standardowej praktyki klinicznej zainteresowanego państwa członkowskiego;
b) decyzja o przepisaniu badanego produktu leczniczego jest podejmowana łącznie z decyzją o włączeniu uczestnika do badania biomedycznego lub
c) oprócz standardowej praktyki klinicznej u uczestników wykonuje się dodatkowe procedury diagnostyczne lub procedury monitorowania.

W ramach przydziału uczestnika, o którym mowa w podpunkcie a), może dochodzić do zautomatyzowanego podejmowania decyzji o skutku prawnym lub w podobnie istotny sposób wpływającym na osobę, której dane dotyczą. W takim przypadku, aby móc przetwarzać te dane, administrator musi pozyskać wyraźną zgodę lub wykazać, że przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym.

4. Obowiązki administratora wynikające z wykorzystywania profilowania obejmującego zautomatyzowane podejmowanie decyzji w badaniach klinicznych

Uznając, że badania kliniczne obejmują przetwarzanie, o którym mowa w art. 22 RODO, administrator danych powinien:

– poinformować o profilowaniu i zasadach zautomatyzowanych decyzji podejmowanych na jego podstawie (art. 13–15);
– poinformować o możliwości wyrażenia sprzeciwu na profilowanie (art. 21);
– poinformować o możliwości kwestionowania automatycznych decyzji wydanych w oparciu na profilowaniu (art. 22);
– przeprowadzić ocenę skutków profilowania dla ochrony danych osobowych (art. 35 ust. 3 lit. a)[57].

[55] *M. Hildebrandt*, The Dawn…, s. 47.

[56] Zgodnie z rozporządzeniem 536/2014 badanie biomedyczne „oznacza każde badanie dotyczące ludzi, mające na celu:

a) odkrycie lub potwierdzenie klinicznych, farmakologicznych lub innych farmakodynamicznych skutków jednego lub większej liczby produktów leczniczych;

b) stwierdzenie wszelkich działań niepożądanych jednego lub większej liczby produktów leczniczych; lub

c) zbadanie wchłaniania, dystrybucji, metabolizmu i wydalania jednego lub większej liczby produktów leczniczych; mające na celu upewnienie się co do bezpieczeństwa lub skuteczności tych produktów leczniczych".

[57] *X. Konarski*, Profilowanie danych osobowych…, s. 50.

Jednym z najbardziej rozbudowanych obowiązków wynikających z RODO w stosunku do polskiej ustawy o ochronie danych osobowych jest obowiązek informacyjny, który administrator powinien spełnić zarówno, jeśli pozyskuje je od osoby, której dane dotyczą (art. 13 RODO), jak i jeśli pozyskuje je w sposób inny niż od osoby, której dane dotyczą (art. 14 RODO). W ramach obowiązku informacyjnego administrator jest zobligowany poinformować m.in. o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu[58]. Ponadto powinien wskazać istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą[59]. Ponadto mimo że nie zostało to wprost wskazane, to w przypadku profilowania kwalifikowanego, administrator powinien poinformować o możliwości kwestionowania decyzji wydanej na podstawie zautomatyzowanego przetwarzania, o którym mowa w art. 22 RODO.

Kwestią dyskusyjną pozostaje, czy należy informować o profilowaniu zwykłym, skoro RODO nie nakłada takiego obowiązku. W art. 13 oraz 14 RODO w zakresie informowania o profilowaniu z art. 4 pkt 4 RODO nie przewidziano analogicznego obowiązku, aczkolwiek motyw 60 RODO wskazuje, że zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania. Motyw nie wskazuje, czy chodzi o profilowanie zwykłe czy kwalifikowane. Jednakże przekazywanie w ramach obowiązku informacyjnego, że przetwarzanie obejmuje profilowanie zwykłe, należy uznać to za dobrą praktykę przyczyniającą się, do pełniejszej realizacji zasady transparentności przetwarzania danych osobowych, zwłaszcza że w przypadku badań klinicznych profilowaniu podlegają szczególne kategorie danych, co ma wpływ na wzrost ryzyka takiego przetwarzania dla praw i wolności osób, których dane dotyczą.

Artykuł 21 ust. 1 RODO stanowi, że osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, tym profilowania na podstawie tych przepisów. Sprzeciw ten ma charakter względnie skuteczny, gdyż administrator może go zakwestionować, jeśli wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Jedyną sytuacją, w której administrator musi bezwzględnie respektować sprzeciw podmiotu danych, jest ta, gdy dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego. Rozporządzenie wprost wskazuje, że jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Należy zauważyć, że zgodnie z art. 21 RODO sprzeciw dotyczy przetwarzania na podstawie art. 6 ust. 1 lit. e) lub f). Wobec czego nie będzie miał zastosowania w przypadku profilowania (zwykłego oraz kwalifikowanego) obejmującego dane wrażliwe. Jedynie sprzeciw na przetwarzanie danych wrażliwych na potrzeby marketingu bezpośredniego będzie mógł zostać skutecznie wniesiony i bezwzględnie respektowany przez administratora danych. Jeśli jednak sponsor będzie przetwarzał dane zwykłe na podstawie art. 6 ust. 1 lit. d) lub f) RODO, wtedy zarówno sprzeciw z art. 21 ust. 1, jak i z ust. 2 RODO będzie przysługiwał osobom, których dane dotyczą.

Ocena skutków dla ochrony danych na gruncie RODO jest wymagana w ściśle określonych przypadkach. W wytycznych Grupy Roboczej dotyczących oceny skutków dla ochrony danych wskazuje się na dziewięć kryteriów, które należy brać pod uwagę, badając, czy dane rodzaj przetwarzania może powodować wysokie ryzyko dla ochrony praw i wolności podmiotu danych. Wśród tych kryteriów znajdują się m.in. dokonywanie oceny lub punktacji, automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku, przetwarzanie danych wrażliwych, przetwarzanie danych na dużą skalę, łączenie lub dopasowywanie zbiorów danych czy przetwarzanie danych dotyczących osób wymagających szczególnej opieki[60].

Z uwagi na to, że w ramach badań klinicznych dochodzi do przetwarzania spełniającego co najmniej dwa z powyższych kryteriów, np. przetwarzania szczególnych kategorii danych na dużą skalę, administrator przed przeprowadzeniem takich badań będzie zobligowany do dokonania oceny skutków dla ochrony danych osobowych. Takie stanowisko dotyczące przeprowadzania oceny skutków w odniesieniu do badań klinicznych zostało dodatkowo poparte przez GIODO w opublikowanym 28.3.2018 r. dokumencie „Proponowany

[58] Jak słusznie zauważa *Mireille Hildebrandt*, dopóki osoba, której dane dotyczą, nie jest świadoma, że została poddana takiej decyzji, nie ma również świadomości o prawach jej przysługujących, np. prawie do zakwestionowania takiej decyzji: *M. Hildebrandt*, Profiling and the rule of law, https://link.springer.com/ content/pdf/10.1007%2Fs12394-008-0003-1.pdf, s. 65 (dostęp z 21.4.2018 r.).

[59] *G. Comande*, *G. Malgieri*, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, International Data Privacy Law 2017 Nr 4, s. 264–265.

[60] Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 (WP 248 rev.01), s. 11–12.

wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków". Organ wskazał w nim, że w jednym z potencjalnych obszarów wystąpienia konieczności takiej oceny będzie prowadzenie badań klinicznych przez szpitale lub inne organizacje[61].

Podsumowanie

Analizując wpływ przepisów RODO na prowadzenie badań klinicznych, należy zauważyć, że akt ten wprowadza inne niż zgoda podstawy przetwarzania danych osobowych uczestników badań klinicznych, np. art. 9 ust. 2 lit. i) RODO legalizujący przetwarzanie niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, czy też art. 9 ust. 2 lit. j) RODO wskazujący na niezbędność przetwarzania danych wrażliwych do celów prowadzenia badań naukowych. Ponadto RODO wprowadza wiele nowych praw i obowiązków, w tym rozbudowany obowiązek informacyjny, ocenę skutków dla ochrony danych, uprzednie konsultacje i inne, z którymi będą mierzyć się administratorzy danych osobowych. Dodatkowo niektóre z praw przysługujących podmiotom danych, np. prawo do przenoszenia danych osobowych, otwierają dyskusję o aktualności dotychczasowego określania ról podmiotów przetwarzających dane osobowe pacjentów (np. koncepcja uznania sponsora za stronę trzecią – co jest jednak dyskusyjne), w tym rozszerza ją o nowe możliwości (np. współadministrowania danymi osobowymi przez sponsora, badacza i ośrodek badawczy). Niewątpliwie konieczność dostosowania się do nowych przepisów przez sponsorów, badaczy i ośrodki, jak też inne podmioty uczestniczące w badaniach klinicznych (np. CRO) wymusi uporządkowanie zasad i procedur przetwarzania danych osobowych w ramach prowadzenia badań klinicznych, tak aby zapewnić realizację praw podmiotów danych i właściwe spełnienie obowiązków przez podmioty przetwarzające dane osobowe.

[64] Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych, https://giodo.gov.pl/pl/file/13366, s. 2 (dostęp z 21.4.2018 r.).

Słowa kluczowe: ochrona danych osobowych, RODO, profilowanie, badania kliniczne, prawo.

Clinical trials in the light of GDPR

Applied in practice models of protection of natural persons in regard to processing of their personal data in clinical trials raise many legal doubts. The issue requires explanation in the light of regulation from the European Parliament and of the Council 2016/679 of 27.4.2016, in the matter of free movement of such data and repealing the directive 95/46/EC. In the present publication the authors attempt to justify interpretation of GDPR regulations which allows to conduct clinical trials in Poland. They point out issues of profiling participants of clinical trials and researchers and other members of a research group, because it is one of the issues that currently raises the most practical problems.

Keywords: personal data protection, GDPR, profiling, clinical trials, law.