



Ministerstwo Cyfryzacji

Departament Zarządzania Danymi
Zastępca Dyrektora
Agnieszka Kułakowska

DZD.WPDO.592.4.2026
Warszawa, 10 sierpnia 2026 r.

Szanowna Pani
Magdalena Zaraś
Zastępca Dyrektora Departamentu Społeczeństwa Obywatelskiego
Kancelaria Prezesa Rady Ministrów

Szanowna Pani Dyrektor,

w związku z przekazaną do Ministerstwa Cyfryzacji uchwałą nr 208 Rady Działalności Pożytku Publicznego z dnia 22 lipca 2026 r. w sprawie propozycji zmian dotyczących stosowania przepisów o ochronie danych osobowych przez organizacje pozarządowe oraz kontynuacji prac nad ich wypracowaniem uprzejmie informuję, że przedstawione w niej postulaty zostały przeanalizowane w zakresie właściwości Ministerstwa Cyfryzacji.

Należy wskazać, że zasadnicza część propozycji zawartych w uchwale dotyczy obowiązków wynikających bezpośrednio z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, zwanego dalej „RODO”. RODO jest rozporządzeniem unijnym, które obowiązuje bezpośrednio we wszystkich państwach członkowskich i nie wymaga transpozycji do prawa krajowego. Przepisy krajowe nie mogą zatem wyłączać ani modyfikować obowiązków ustanowionych w RODO, poza przypadkami, w których samo rozporządzenie wyraźnie pozostawia państwom członkowskim możliwość przyjęcia regulacji krajowych.

Zmiany o charakterze strukturalnym dotyczące systemu ochrony danych osobowych ustanowionego w RODO wymagają działania na poziomie Unii Europejskiej, przy czym Komisja Europejska posiada inicjatywę prawodawczą w tym zakresie. Jednocześnie na forum Unii Europejskiej toczą się obecnie prace nad wnioskiem Komisji Europejskiej w ramach pakietu legislacyjnego określanego jako „Omnibus Cyfrowy”, obejmujące również propozycje dotyczące uproszczenia niektórych obowiązków wynikających z RODO.

Odnosząc się kolejno do poszczególnych postulatów zawartych w § 1 ust. 2 uchwały nr 208, należy wskazać, co następuje:

Ad 1. Wprowadzenie klasyfikacji organizacji pozarządowych aby zwolnić z części obowiązków mikro i małe podmioty.

Postulat ten nie odpowiada przyjętemu w RODO podejściu opartemu na ryzyku (risk-based approach). Zakres obowiązków administratora jest bowiem uzależniony przede wszystkim od charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych, a nie wyłącznie od formy prawnej, statusu czy wielkości organizacyjnej administratora. Sam fakt prowadzenia działalności w niewielkiej skali organizacyjnej nie oznacza automatycznie, że dany podmiot przetwarza dane osobowe na niewielką skalę albo że przetwarzanie to powoduje niskie ryzyko. Organizacja pozarządowa, także dysponująca ograniczonym personelem lub budżetem, może przetwarzać znaczne ilości danych, dane szczególnych kategorii, dane osób wymagających

szczegółnej ochrony albo prowadzić operacje przetwarzania wiążące się z podwyższonym ryzykiem. Z tego względu sama kwalifikacja organizacji do kategorii mikro, małych albo średnich nie może stanowić podstawy do generalnego wyłączenia lub ograniczenia obowiązków wynikających z RODO.

Odnosząc się natomiast do samego postulatu wprowadzenia klasyfikacji organizacji pozarządowych według skali prowadzonej działalności, należy zauważyć, że ewentualne ustanowienie takiej klasyfikacji wymagałoby zmian w ustawie z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie, która nie pozostaje w zakresie właściwości Ministerstwa Cyfryzacji. Propozycje odnoszące się do systemowego podziału organizacji pozarządowych na mikro, małe, średnie i duże powinny zatem zostać rozpatrzone przez organ właściwy w sprawach tej ustawy. Niezależnie od powyższego wprowadzenie takiej klasyfikacji w prawie krajowym nie mogłoby samo w sobie stanowić podstawy do wyłączenia albo ograniczenia obowiązków wynikających bezpośrednio z RODO.

Ad 2. Uproszczenie obowiązków dokumentacyjnych i informacyjnych.

W odniesieniu do postulatu uproszczenia obowiązków dokumentacyjnych, w szczególności obowiązków informacyjnych, prowadzenia rejestru czynności przetwarzania oraz dokumentacji ochrony danych osobowych, należy wskazać, że obowiązki informacyjne określone w art. 13 i 14 RODO służą zapewnieniu przejrzystości przetwarzania danych oraz realizacji prawa osoby fizycznej do uzyskania informacji o sposobie wykorzystywania jej danych. Prawo krajowe nie może wprowadzić generalnego zwolnienia organizacji pozarządowych z tych obowiązków ani ograniczyć ich ze względu na wielkość albo formę prawną administratora.

RODO przewiduje określone przypadki, w których przekazanie poszczególnych informacji nie jest wymagane albo w których obowiązek informacyjny może zostać ograniczony. Możliwości te wynikają jednak bezpośrednio z przepisów RODO i są związane z konkretnymi okolicznościami przetwarzania, a nie z przynależnością administratora do określonej kategorii podmiotów. Ewentualne ograniczenia praw i obowiązków przewidzianych w RODO mogą być ustanawiane wyłącznie na warunkach określonych w RODO, w szczególności z poszanowaniem istoty podstawowych praw i wolności oraz przy zastosowaniu niezbędnych, równoważnych i proporcjonalnych zabezpieczeń.

RODO już obecnie uwzględnia potrzebę ograniczania obciążeń administracyjnych mniejszych podmiotów. Przykładowo art. 30 ust. 5 RODO przewiduje wyjątek od obowiązku prowadzenia rejestru czynności przetwarzania przez przedsiębiorstwo lub podmiot zatrudniający mniej niż 250 osób. Wyjątek ten nie ma jednak zastosowania, jeżeli przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, nie ma charakteru sporadycznego albo obejmuje dane szczególnych kategorii lub dane dotyczące wyroków skazujących i naruszeń prawa. Konstrukcja tego przepisu potwierdza, że zakres obowiązków dokumentacyjnych zależy nie tylko od wielkości podmiotu, lecz również od skali, charakteru i ryzyka związanego z przetwarzaniem.

RODO nie ustanawia sztywnego, sformalizowanego katalogu dokumentów, które administrator danych musi posiadać. Przeciwnie - przyjmuje model oparty na elastyczności i ww. podejściu opartym na ryzyku (risk-based approach), pozostawiając administratorowi znaczną swobodę w doborze środków organizacyjnych i sposobu dokumentowania zgodności z przepisami. Kluczowe znaczenie ma w tym zakresie zasada rozliczalności, wyrażona w art. 5 ust. 2 RODO. Zgodnie z nią administrator jest nie tylko zobowiązany do przestrzegania zasad przetwarzania danych osobowych, lecz również do wykazania, że

zasady te są przestrzegane. RODO nie narzuca jednak jednolitego modelu realizacji tego obowiązku. To administrator, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz poziomu ryzyka dla praw i wolności osób fizycznych, decyduje, jakie procedury czy inne środki dokumentacyjne będą adekwatne do prowadzonej działalności. W praktyce oznacza to, że niewielka organizacja pozarządowa przetwarzająca ograniczony zakres danych może już obecnie prowadzić i posiadać znacznie prostszą dokumentację niż duży podmiot publiczny lub przedsiębiorca prowadzący przetwarzanie na szeroką skalę.

Zakres obowiązków administratora wynika bezpośrednio z rozporządzenia unijnego, które jako akt o bezpośrednim stosowaniu ma pierwszeństwo przed prawem krajowym. Państwo członkowskie nie jest uprawnione do ograniczania ani modyfikowania tych obowiązków wynikających z RODO poza przypadkami wyraźnie przewidzianymi w samym RODO. Oznacza to, że ustawodawca krajowy nie może zwolnić określonej kategorii administratorów z obowiązków wynikających z zasady rozliczalności ani ustanowić standardu ochrony niższego od wymaganego przez prawo Unii Europejskiej.

Analogicznie należy ocenić propozycję ograniczenia obowiązków informacyjnych. Obowiązki określone w art. 13 i 14 RODO stanowią jeden z podstawowych mechanizmów realizacji zasady przejrzystości oraz prawa osoby, której dane dotyczą, do uzyskania informacji o przetwarzaniu jej danych osobowych. Dzięki nim osoba fizyczna uzyskuje wiedzę o tym, kto jest administratorem danych, w jakim celu i na jakiej podstawie prawnej dane są przetwarzane, jak długo będą przechowywane, komu mogą zostać udostępnione oraz jakie prawa przysługują jej w związku z przetwarzaniem. Obowiązki te nie mają charakteru wyłącznie formalnego, lecz stanowią jedną z podstawowych gwarancji skutecznego wykonywania praw wynikających z RODO oraz realizacji zasady przejrzystości przetwarzania danych.

Możliwość ustawowego ograniczenia praw i obowiązków przewidzianych w RODO została uregulowana w art. 23 RODO i ma charakter wyjątkowy. Ograniczenia mogą zostać wprowadzone jedynie w drodze przepisów prawa, wyłącznie wtedy, gdy są konieczne i proporcjonalne dla ochrony ściśle określonych wartości, takich jak bezpieczeństwo narodowe, obronność, bezpieczeństwo publiczne, zapobieganie i ściganie przestępstw czy inne istotne cele interesu publicznego wskazane w tym przepisie. Katalog ten ma charakter zamknięty i podlega ścisłej wykładni. Trudno zatem uznać, aby typowa działalność organizacji pozarządowych mieściła się w zakresie przesłanek uzasadniających wprowadzenie takich ograniczeń.

Ad 3. Uznanie polityki ochrony danych za podstawowy dokument.

RODO nie ustanawia zamkniętego katalogu dokumentów, które każdy administrator musi prowadzić w identycznej formie. Zgodnie z zasadą rozliczalności administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne oraz być w stanie wykazać zgodność przetwarzania z przepisami. Zakres i sposób dokumentowania tych działań powinny odpowiadać charakterowi, zakresowi, kontekstowi i celom przetwarzania oraz występującemu ryzyku. Już obecna konstrukcja RODO pozwala zatem mniejszym organizacjom dostosować zakres dokumentacji do rzeczywistych okoliczności ich działalności, nie zwalniając ich jednak z obowiązku zapewnienia i wykazania zgodności przetwarzania z prawem.

Z tych samych względów nie znajduje uzasadnienia ustawowe uznanie polityki ochrony danych za jeden podstawowy dokument opisujący sposób zapewnienia zgodności z RODO. RODO nie wymaga przyjęcia dokumentu o określonej nazwie ani nie przewiduje, aby posiadanie jednego dokumentu mogło zastępować realizację poszczególnych

obowiązków administratora. Dobór dokumentacji powinien pozostawać dostosowany do działalności danego administratora oraz prowadzonych operacji przetwarzania. Sama polityka ochrony danych może stanowić element systemu zapewnienia zgodności, nie może jednak zastępować innych dokumentów lub działań wymaganych w konkretnym przypadku, takich jak rejestr czynności przetwarzania, analiza ryzyka, ocena skutków dla ochrony danych, dokumentacja naruszeń czy wykazanie prawidłowego wykonania obowiązków informacyjnych.

Postulat uznania polityki ochrony danych za podstawowy dokument potwierdzający zgodność organizacji z przepisami RODO opiera się na błędnym założeniu, że zgodność z regulacjami dotyczącymi ochrony danych osobowych może zostać sprowadzona do posiadania jednego, formalnie określonego dokumentu. Tymczasem konstrukcja RODO opiera się na całkowicie odmiennym modelu - ochrona danych osobowych została ujęta jako proces ciągłego zarządzania ryzykiem, a nie tylko jako obowiązek sporządzenia i utrzymywania określonej dokumentacji.

Należy podkreślić, że kwestia wdrażania polityk ochrony danych została już uregulowana w art. 24 ust. 2 RODO. Przepis ten przewiduje możliwość wdrożenia odpowiednich polityk przez administratora, jednak wyłącznie w zakresie, w jakim jest to proporcjonalne do charakteru prowadzonego przetwarzania. Oznacza to, że samo RODO pozostawia administratorowi swobodę w doborze narzędzi organizacyjnych służących zapewnieniu zgodności z prawem, kierując się zasadą proporcjonalności oraz ww. podejściem opartym na ryzyku. RODO nie ustanawia polityki ochrony danych jako dokumentu obowiązkowego dla każdego administratora ani tym bardziej nie przypisuje jej szczególnego statusu jako dokumentu nadrzędnego wobec innych środków organizacyjnych. Tym samym sam prawodawca unijny pozostawił administratorom swobodę doboru polityk i dokumentacji odpowiednich do charakteru prowadzonego przetwarzania, co wyklucza potrzebę ustawowego wskazywania jednego dokumentu jako podstawowego środka wykazywania zgodności z RODO.

Z tego względu próba ustawowego uznania polityki ochrony danych za podstawowy dokument potwierdzający zgodność z przepisami prowadziłaby do wypaczenia modelu przyjętego przez prawodawcę unijnego. Ochrona danych osobowych nie jest bowiem oceniana przez pryzmat posiadania określonych dokumentów, lecz przez pryzmat rzeczywiście wdrożonych u administratora rozwiązań organizacyjnych i technicznych oraz ich skuteczności. Zgodnie z art. 24 ust. 1 RODO administrator jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych oraz do ich regularnego przeglądu i aktualizacji, tak aby przetwarzanie odbywało się zgodnie z wymaganiami RODO. Dokumentacja pełni w tym modelu jedynie funkcję pomocniczą - ma odzwierciedlać faktycznie funkcjonujący system ochrony danych, a nie zastępować jego rzeczywiste elementy.

Jeszcze wyraźniej wynika to z art. 32 RODO, który nakłada obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania. Ocena zgodności z tym przepisem nie opiera się na analizie treści polityki ochrony danych, lecz na weryfikacji, czy administrator rzeczywiście stosuje adekwatne zabezpieczenia, uwzględniające stan wiedzy technicznej, koszty wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych. Analogicznie ocenie podlega realizacja pozostałych zasad wynikających z art. 5 RODO, w szczególności zasady minimalizacji danych, ograniczenia celu czy integralności i poufności. Żadna z tych zasad nie może zostać uznana za spełnioną wyłącznie z uwagi na fakt posiadania polityki ochrony danych.

Przyjęcie rozwiązania, zgodnie z którym posiadanie polityki ochrony danych prowadziłoby do ograniczenia innych obowiązków formalnych lub stanowiłoby domniemanie zgodności z RODO, mogłoby prowadzić do utrwalenia modelu zgodności polegającego wyłącznie na formalnym spełnianiu wymogów dokumentacyjnych („tick-box compliance”), zamiast na rzeczywistym zarządzaniu bezpieczeństwem danych. Takie podejście pozostaje w sprzeczności z duchem RODO, który odchodzi od sztywnego formalizmu charakterystycznego dla wcześniejszych regulacji na rzecz odpowiedzialności administratora za skuteczność stosowanych środków ochrony danych.

Ad 4. Przegląd obowiązków dotyczących upoważnień i oświadczeń.

Postulat dokonania przeglądu obowiązków dotyczących upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu poufności wymaga rozróżnienia pomiędzy obowiązkami wynikającymi bezpośrednio z RODO a rozwiązaniami organizacyjnymi przyjmowanymi przez administratorów lub przewidzianymi w niektórych przepisach prawa krajowego. W praktyce bowiem znaczna część obowiązków postrzeganych jako nadmiernie sformalizowane nie wynika z samego RODO, lecz z utrwalonych praktyk organizacyjnych albo z regulacji sektorowych obowiązujących w określonych obszarach działalności.

Art. 29 oraz art. 32 ust. 4 RODO określają obowiązki o charakterze funkcjonalnym. Wymagają one, aby każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego przetwarzała dane wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek przetwarzania wynika z przepisów prawa. Jednocześnie administrator zobowiązany jest zapewnić, aby osoby mające dostęp do danych były zobowiązane do zachowania ich poufności lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. RODO nie przesądza jednak o formie realizacji tych obowiązków, pozostawiając administratorowi swobodę w zakresie doboru odpowiednich środków organizacyjnych.

Oznacza to, że praktyka polegająca na wydawaniu pisemnych upoważnień oraz odbieraniu odrębnych oświadczeń o zachowaniu poufności stanowi jedynie jeden z możliwych sposobów wykazania zgodności z przepisami. Administrator może osiągnąć ten sam cel za pomocą innych rozwiązań organizacyjnych, takich jak odpowiednie zapisy w umowach o pracę, umowach cywilnoprawnych, regulaminach wewnętrznych, elektronicznych systemach nadawania uprawnień czy procedurach zarządzania dostępem do danych. Istotne znaczenie ma bowiem nie sama forma dokumentowania uprawnień, lecz możliwość wykazania, że dostęp do danych posiadają wyłącznie osoby do tego upoważnione oraz że zakres ich uprawnień odpowiada wykonywanym obowiązkom.

Jednocześnie nie ulega wątpliwości, że sam obowiązek sprawowania kontroli nad dostępem do danych osobowych ma charakter fundamentalny i wynika bezpośrednio z RODO. Administrator powinien posiadać wiedzę, które osoby - niezależnie od podstawy współpracy, czy są to pracownicy, wolontariusze, członkowie organów organizacji czy współpracownicy wykonujący zadania na podstawie umów cywilnoprawnych - mają dostęp do danych osobowych, w jakim zakresie oraz na jakiej podstawie. Obowiązek ten pozostaje w ścisłym związku z zasadą integralności i poufności określoną w art. 5 ust. 1 lit. f RODO oraz z obowiązkiem wdrożenia odpowiednich środków technicznych i organizacyjnych przewidzianym w art. 32 RODO.

Postulat dokonania przeglądu obowiązków wynikających z przepisów dotyczących upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu poufności dotyczy też częściowo regulacji prawa krajowego. W Ministerstwie Cyfryzacji

analizowane są możliwości uproszczenia i uelastycznienia sposobu udzielania oraz dokumentowania upoważnień do przetwarzania danych osobowych, przy jednoczesnym zachowaniu wymogów wynikających z RODO oraz możliwości jednoznacznego ustalenia osoby upoważnionej, zakresu jej uprawnień, a także momentu ich nadania i cofnięcia. Analizy te zmierzają w szczególności do oceny, czy obowiązujące regulacje krajowe nie ustanawiają nadmiernych wymagań formalnych i czy możliwe jest szersze wykorzystanie rozwiązań organizacyjnych i systemowych, w tym nadawania odpowiednich uprawnień w systemach teleinformatycznych. Analizy te prowadzone są jednak z uwzględnieniem potrzeb wszystkich administratorów danych osobowych i nie są ograniczone wyłącznie do organizacji pozarządowych.

Ad 5. Ograniczenie wysokości administracyjnych kar pieniężnych dla NGO.

Nie jest możliwe wprowadzenie generalnego ograniczenia wysokości administracyjnych kar pieniężnych nakładanych na organizacje pozarządowe przez objęcie ich szczególnym, preferencyjnym reżimem odpowiedzialności. System administracyjnych kar pieniężnych został uregulowany w art. 83 RODO. Przy podejmowaniu decyzji o nałożeniu kary oraz ustalaniu jej wysokości organ nadzorczy ma obowiązek uwzględnić wszystkie okoliczności konkretnej sprawy, w tym charakter, wagę i czas trwania naruszenia, umyślny lub nieumyślny charakter naruszenia, działania podjęte w celu zminimalizowania szkody, stopień odpowiedzialności administratora, jego wcześniejsze naruszenia, poziom współpracy z organem nadzorczym oraz kategorie danych, których dotyczyło naruszenie.

Mechanizm ten pozwala uwzględnić rzeczywistą sytuację konkretnej organizacji oraz zapewnić, aby kara była w każdym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca. RODO nie przewiduje natomiast możliwości ustanowienia w prawie krajowym generalnego, obniżonego limitu administracyjnych kar pieniężnych dla organizacji pozarządowych jako odrębnej kategorii administratorów. Organizacje te nie stanowią też jednolitej grupy pod względem charakteru prowadzonej działalności, w tym działalności gospodarczej, skali przetwarzania danych ani sytuacji ekonomicznej. W konsekwencji brak jest podstaw do ich uprzywilejowania względem innych administratorów przez wprowadzenie odrębnego, niższego limitu administracyjnych kar pieniężnych. Mikro, małe i średnie przedsiębiorstwa również nie mają i nie mogą mieć takiego specjalnego ograniczenia.

Jednocześnie należy podkreślić, że art. 83 ust. 2 RODO zobowiązuje organ nadzorczy do każdorazowego uwzględnienia wszystkich okoliczności konkretnej sprawy przy wymiarze administracyjnej kary pieniężnej. Pozwala to na właściwe uwzględnienie specyfiki działalności administratora, skali prowadzonej działalności oraz pozostałych okoliczności mających znaczenie dla oceny proporcjonalności kary. Obowiązujące obecnie przepisy RODO zapewniają zatem możliwość indywidualizacji rozstrzygnięcia bez potrzeby tworzenia odrębnego reżimu odpowiedzialności dla organizacji pozarządowych.

Ad 6. Opracowanie wytycznych, standardów i wzorów przez Prezesa UODO.

W odniesieniu do postulatu opracowania przez Prezesa Urzędu Ochrony Danych Osobowych wytycznych, standardów oraz wzorów dokumentów należy wskazać, że Prezes UODO jest w pełni niezależnym organem nadzorczym. Minister Cyfryzacji nie posiada kompetencji do zobowiązywania Prezesa UODO do opracowania określonych wytycznych, standardów, formularzy ani wzorów dokumentów. Wynika to z ustrojowej niezależności organów nadzorczych gwarantowanej w art. 52 ust. 1 i 2 RODO.

Do zadań organu nadzorczego należy między innymi upowszechnianie wiedzy o obowiązkach administratorów i podmiotów przetwarzających oraz zwiększanie świadomości w zakresie ryzyka, przepisów, zabezpieczeń i praw związanych z przetwarzaniem danych. O sposobie realizacji tych zadań, w tym o wyborze zagadnień wymagających wydania wytycznych albo przygotowania materiałów przeznaczonych dla określonych grup administratorów, rozstrzyga samodzielnie Prezes UODO.

Zgodnie z art. 52 ust. 1 i 2 RODO organy nadzorcze wykonują swoje zadania w pełni niezależnie i pozostają wolne od zewnętrznych wpływów. Ministerstwo Cyfryzacji nie jest zatem uprawnione do wyznaczania Prezesowi UODO kierunków działań informacyjnych lub edukacyjnych ani zobowiązywania go do opracowania określonych standardów, wytycznych lub wzorów dokumentów. Postulat dotyczący przygotowania materiałów przeznaczonych dla organizacji pozarządowych może być zatem kierowany bezpośrednio do organu nadzorczego, jednak Minister Cyfryzacji nie może przesądzić o jego realizacji ani o zakresie ewentualnych wytycznych.

Ad 7. Uproszczenie zasad weryfikacji podmiotów przetwarzających.

Odnosząc się do propozycji uproszczenia zasad weryfikacji podmiotów przetwarzających oraz opracowania jednolitych standardów w tym zakresie, należy zauważyć, że zgodnie z art. 28 RODO administrator może korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Ocena tych gwarancji musi uwzględniać charakter konkretnej usługi, rodzaj danych, zakres i cele powierzonego przetwarzania, stosowane zabezpieczenia oraz związane z nim ryzyko. Nie jest zatem możliwe ustanowienie jednego uproszczonego sposobu weryfikacji, który byłby wystarczający we wszystkich przypadkach. Inny zakres oceny może być odpowiedni przy korzystaniu ze standardowej usługi technicznej obejmującej ograniczony zakres danych, a inny w przypadku powierzenia przetwarzania danych szczególnych kategorii, danych dzieci albo dużych zbiorów danych.

Pomocnicze standardy, listy kontrolne, kodeksy postępowania lub mechanizmy certyfikacji mogą ułatwiać administratorom ocenę podmiotów przetwarzających, nie mogą jednak zastąpić indywidualnej oceny wymaganej na podstawie art. 28 RODO ani przeniesić odpowiedzialności administratora na inny podmiot. Ewentualne materiały interpretacyjne lub praktyczne w tym zakresie pozostają przede wszystkim w obszarze działalności niezależnego organu nadzorczego, organizacji branżowych albo podmiotów opracowujących kodeksy postępowania i mechanizmy certyfikacji przewidziane w RODO.

Obowiązek zachowania należytej staranności przy wyborze podmiotu przetwarzającego wynika bezpośrednio z art. 28 ust. 1 RODO i stanowi jeden z podstawowych mechanizmów zapewnienia bezpieczeństwa danych osobowych w relacjach outsourcingowych. Administrator ponosi odpowiedzialność za dokonanie świadomego wyboru procesora oraz za ocenę, czy wybrany podmiot rzeczywiście daje rękojmię zgodnego z prawem i bezpiecznego przetwarzania danych.

Szczególne znaczenie obowiązek ten ma również w działalności organizacji pozarządowych, które często korzystają z usług zewnętrznych podmiotów świadczących obsługę księgową, usługi informatyczne, hosting, przechowywanie danych w chmurze, platformy do prowadzenia zbiorów czy narzędzia do komunikacji z darczyńcami i wolontariuszami. Dane powierzane takim podmiotom obejmują nierzadko informacje

dotyczące darczyńców, beneficjentów pomocy, wolontariuszy lub członków organizacji, a w wielu przypadkach również szczególne kategorie danych osobowych. Z tego względu obowiązek uprzedniej weryfikacji procesora stanowi istotny element systemu ochrony tych osób i nie może być traktowany wyłącznie jako wymóg o charakterze formalnym.

Jednocześnie należy podkreślić, że RODO nie narzuca administratorom jednolitej metody przeprowadzania takiej weryfikacji. Rozporządzenie nie wymaga stosowania rozbudowanych procedur audytowych ani sporządzania określonych formularzy czy raportów. Zakres działań weryfikacyjnych powinien być dostosowany do charakteru i skali przetwarzania oraz poziomu ryzyka dla praw i wolności osób fizycznych. W praktyce administrator może oprzeć ocenę procesora na analizie przedstawionych środków bezpieczeństwa, weryfikacji posiadanych certyfikatów, stosowanych standardów bezpieczeństwa, przystąpienia do zatwierdzonych kodeksów postępowania, wyników audytów lub informacji uzyskanych od podmiotu przetwarzającego. W przypadku niewielkich organizacji pozarządowych zakres tej weryfikacji może być odpowiednio uproszczony, o ile pozostaje adekwatny do poziomu ryzyka związanego z powierzonym przetwarzaniem.

Elastyczność przewidziana w RODO oznacza zatem, że administrator samodzielnie dobiera sposób realizacji obowiązku wynikającego z art. 28 ust. 1, kierując się zasadą proporcjonalności i ww. podejściem opartym na ryzyku. Nie oznacza to jednak możliwości całkowitego odstąpienia od weryfikacji podmiotu przetwarzającego. Zwolnienie organizacji pozarządowych z obowiązku oceny, czy procesor zapewnia odpowiedni poziom ochrony danych, prowadziłoby do obniżenia standardu bezpieczeństwa danych osobowych oraz pozostawałoby w sprzeczności z podstawowymi założeniami systemu odpowiedzialności administratora przyjętego przez prawodawcę unijnego. Ewentualne działania mające na celu ułatwienie administratorom realizacji tego obowiązku mogą polegać na opracowywaniu materiałów pomocniczych lub dobrych praktyk przez organ nadzorczy, nie mogą jednak prowadzić do ograniczenia obowiązków wynikających bezpośrednio z art. 28 RODO.

Ad 8. Wydłużenie terminu zgłoszenia naruszenia ochrony danych osobowych.

Termin zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu wynika bezpośrednio z art. 33 ust. 1 RODO i wynosi, o ile jest to wykonalne, nie później niż 72 godziny po stwierdzeniu naruszenia. Termin ten nie może zostać wydłużony w przepisach prawa krajowego ani odmiennie określony wyłącznie dla organizacji pozarządowych.

Należy jednocześnie podkreślić, że obowiązek zgłoszenia nie dotyczy każdego naruszenia ochrony danych osobowych. Zgłoszenie nie jest wymagane, jeżeli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. RODO przewiduje również, że jeżeli zgłoszenie nie może zostać dokonane w terminie 72 godzin, administrator może przekazać je po tym terminie, podając przyczyny opóźnienia, a informacje mogą być przekazywane sukcesywnie, bez dalszej zbędnej zwłoki.

Ratio legis terminu określonego w art. 33 ust. 1 RODO polega na zapewnieniu możliwie szybkiego podjęcia działań ograniczających ryzyko naruszenia praw lub wolności osób fizycznych. Jednocześnie mechanizm przewidziany w art. 33 ust. 4 RODO pozwala administratorowi uzupełniać informacje przekazane organowi nadzorczemu sukcesywnie, w miarę postępu analiz dotyczących naruszenia.

Zmiana samego terminu wymagałaby jednak zmiany RODO na poziomie Unii Europejskiej. W toku obecnie prowadzonych prac legislacyjnych dotyczących uproszczenia stosowania RODO rozważane jest wydłużenie terminu zgłoszenia naruszenia z 72 do 96 godzin. Ministerstwo Cyfryzacji popiera wydłużenie tego terminu. Postulat Rady w tym zakresie jest zatem uwzględniany w stanowisku prezentowanym przez Polskę na forum Unii Europejskiej, jednak nie może zostać zrealizowany w drodze zmiany przepisów krajowych ani ustanowienia rozwiązania odnoszącego się wyłącznie do organizacji pozarządowych.

Podsumowanie

Podsumowując, postulaty przedstawione w uchwale zostały przeanalizowane w zakresie właściwości Ministerstwa Cyfryzacji. Część z nich dotyczy obowiązków wynikających bezpośrednio z RODO i nie może zostać zrealizowana przez przyjęcie szczególnych regulacji krajowych dla organizacji pozarządowych. Dotyczy to w szczególności generalnego ograniczenia obowiązków informacyjnych i dokumentacyjnych, ustanowienia preferencyjnego systemu administracyjnych kar pieniężnych, uproszczenia obowiązków wynikających z art. 28 RODO oraz wydłużenia w prawie krajowym terminu zgłoszenia naruszenia ochrony danych osobowych.

Propozycja wprowadzenia klasyfikacji organizacji pozarządowych według skali prowadzonej działalności dotyczy natomiast ustawy pozostającej poza właściwością Ministra Cyfryzacji. Z kolei decyzje dotyczące opracowania wytycznych, standardów i wzorów dokumentów należą do niezależnego Prezesa UODO, którego Minister Cyfryzacji nie może zobowiązać do podjęcia wskazanych działań.

W zakresie regulacji krajowych pozostających we właściwości Ministra Cyfryzacji prowadzone są analizy dotyczące możliwości ograniczenia nadmiernego formalizmu związanego z udzielaniem i dokumentowaniem pisemnych upoważnień do przetwarzania danych osobowych. Ewentualne rozwiązania w tym zakresie powinny mieć charakter ogólny, odpowiadać potrzebom wszystkich kategorii administratorów oraz pozostawać zgodne z zasadą rozliczalności i opartym na ryzyku podejściem RODO. Nie jest zasadne wprowadzanie do ustawy o ochronie danych osobowych szczególnych regulacji przeznaczonych wyłącznie dla organizacji pozarządowych.

Odnosząc się do postulatu rozpoczęcia prac w formule wspólnej grupy roboczej, należy wskazać, że przedstawione w uchwale propozycje zostały przeanalizowane w zakresie właściwości Ministerstwa Cyfryzacji, a stanowisko Ministerstwa w odniesieniu do poszczególnych postulatów zostało przedstawione powyżej. Część zgłoszonych propozycji dotyczy materii uregulowanej bezpośrednio w RODO i wymagałaby zmian prawa Unii Europejskiej, część pozostaje poza właściwością Ministerstwa Cyfryzacji, natomiast pozostałe zagadnienia są analizowane w ramach prowadzonych prac analitycznych dotyczących krajowych regulacji z zakresu ochrony danych osobowych. Na obecnym etapie przedstawione postulaty nie uzasadniają potrzeby powoływania specjalnej grupy roboczej w tym zakresie. Ministerstwo Cyfryzacji pozostaje otwarte na wymianę informacji z zainteresowanymi środowiskami w zakresie zagadnień pozostających w jego właściwości.

Z wyrazami szacunku

Agnieszka Kułakowska
/dokument podpisany elektronicznie/