PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa,

DPNT.401.329.2025

Pan
Maciej Berek

Minister nadzoru nad wdrażaniem polityki rządu
Przewodniczący Komitetu Stałego Rady Ministrów

Kancelaria Prezesa Rady Ministrów

Szanowny Panie Ministrze,

w odpowiedzi na korespondencję z 26 sierpnia 2025 r. dotyczącą zmian przepisów w ramach tzw. deregulacji, tj. zmian **ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, ustawy z dnia 9 marca 2023 r. o badaniach klinicznych produktów leczniczych stosowanych u ludzi oraz ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów**, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], Prezes UODO jako organ nadzorczy **zwraca uwagę na następujące kwestie**.

Odnosząc się do proponowanych zmian w zakresie **rezygnacji z pisemnej formy upoważnień do przetwarzania danych osobowych** w następujących regulacjach: art. 22^{1b} § 3 Kodeksu pracy[3], art. 36 ust. 4 ustawy o badaniach klinicznych produktów

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.), dalej także jako: RODO.
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
[3] „Do przetwarzania danych osobowych, o których mowa w § 1, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy."

leczniczych stosowanych u ludzi[4] oraz art. 27 ust. 2 ustawy o ochronie sygnalistów[5], pragnę zwrócić uwagę, że obowiązkiem każdego administratora jest zapewnienie, aby osoba fizyczna, która działa z upoważnienia administratora (oraz podmiotu przetwarzającego), mająca dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego (**art. 32 ust. 4** rozporządzenia 2016/679). Jest to niezwykle ważny aspekt dotyczący zapewnienia przez administratora bezpieczeństwa przetwarzania danych osobowych, tj. określenia właściwego stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem, w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W konsekwencji to administrator określa krąg osób, które mają dostęp do danych i dalszych form ich przetwarzania.

Biorąc pod uwagę treść art. 29 ogólnego rozporządzenia o ochronie danych osobowych[6] podkreślić należy, że **rozporządzenie 2016/679 nie wymaga sformalizowanej konstrukcji pisemnych upoważnień wydawanych przez administratorów jako warunku dopuszczenia danej osoby do przetwarzania danych osobowych**. Prawodawca wymaga faktycznego, a nie jedynie formalnego podniesienia standardu ochrony danych i prawa osób fizycznych – ochrona powinna być rzeczywista i skuteczna. Zatem **pisemne upoważnienie jest środkiem nie wymaganym przez rozporządzenie 2016/679.**

Przepisy ogólnego rozporządzenia o ochronie danych nie wymagają, aby administrator nadawał formalne upoważnienia, jednak prawidłowe stosowanie zasady rozliczalności (art. 5 ust. 2 ww. rozporządzenia[7]) oznacza, że administrator wykazuje prawidłowe wykonywanie obowiązków wynikających z przepisów tego aktu, w tym obowiązek upoważnienia do przetwarzania danych osobowych w odpowiednim zakresie. W rozporządzeniu 2016/679 nie ma definicji pojęcia polecenia przetwarzania wydawanego przez administratora. Prawo administratora do wydawania wiążących poleceń wynika z jego funkcji (art. 4 pkt 7) i jest ściśle powiązane z obowiązkiem stosowania się do nich przez osoby, do których polecenia te są adresowane (art. 29 rozporządzenia 2016/679) oraz zabezpieczone jest zobowiązaniem administratora do

[4] „Sponsor dopuszcza do przetwarzania danych osobowych wyłącznie osoby posiadające pisemne upoważnienie wydane przez administratora danych. Osoby upoważnione do przetwarzania danych osobowych zobowiązują się na piśmie do zachowania ich w tajemnicy."

[5] „Do przyjmowania i weryfikacji zgłoszeń wewnętrznych, podejmowania działań następczych oraz przetwarzania danych osobowych osób, o których mowa w ust. 1, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie podmiotu prawnego. Osoby upoważnione są obowiązane do zachowania tajemnicy w zakresie informacji i danych osobowych, które uzyskały w ramach przyjmowania i weryfikacji zgłoszeń wewnętrznych, oraz podejmowania działań następczych, także po ustaniu stosunku pracy lub innego stosunku prawnego, w ramach którego wykonywały tę pracę."

[6] Zgodnie z art. 29 rozporządzenia 2016/679: „Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego".

[7] „Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność")".

wdrożenia rozwiązań mających zapewnić, aby osoby mające dostęp danych osobowych przetwarzały je jedynie na polecenie administratora (art. 32 ust. 4). Rolą administratora jest więc wyznaczenie poleceniem ram, w jakich mogą się poruszać osoby, którym nadano dostęp do danych osobowych. Sama **forma wyznaczenia przez administratora dostępu do danych czy systemów, w których są one przetwarzane, nie została precyzyjnie określona w przepisach rozporządzenia 2016/679.**

Istotne jest, że to administrator ma obowiązek zorganizowania procesów przetwarzania, aby możliwa była weryfikacja, czy dostęp do danych osobowych nie został nadany osobom nieupoważnionym lub w szerszym zakresie niż jest to konieczne. To on odpowiada za prawidłowe przetwarzanie danych w organizacji. Upoważnienie nadane przez administratora może mieć formę pisemną lub dokumentową, może wynikać z czynności faktycznej. Obecne regulacje krajowe w wielu aktach prawnych[8] zawierają obowiązek udzielania pisemnych upoważnień do przetwarzania najczęściej określonych kategorii danych, lecz są to rozwiązania nadmiarowe. Poza doprecyzowaniem zakresu dostępu do danych **upoważnienia stanowią formę zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą, lub zabezpieczenia zapobiegającego nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu danych osobowych**. Wymóg sformułowania takich zabezpieczeń wynika z art. 9 ust. 2 lit. b oraz art. 23 ust. 2 lit. d rozporządzenia 2016/679. Administrator, który rezygnuje z pisemnej formy upoważnienia powinien być w stanie wykazać (w myśl ww. zasady rozliczalności), że upoważnienia zostały nadane i istnieje rzeczywista kontrola sprawowana przez osoby uprawnione nad danymi osobowymi.

Prawodawca, mający za cel deregulację, rozważyć powinien przeprowadzenie **testu prywatności w procesie tworzenia prawa**, w tym oceny skutków dla ochrony danych – art. 25 ust. 1 rozporządzenia 2016/679, tj. przy określaniu sposobów przetwarzania, jak i art. 35 (w szczególności ust. 1 i ust. 10), tj. w związku z przyjmowaniem podstawy prawnej przetwarzania. Konsekwencją takiej analizy ryzyka powinno być kompleksowe odzwierciedlenie projektowanych zmian w obowiązującym porządku prawnym z uwzględnieniem zasad przetwarzania danych osobowych wynikających z rozporządzenia 2016/679. Jeżeli mocą projektowanych regulacji miałyby być wskazane dodatkowe zabezpieczenia dla ochrony danych, to należy je wskazać konkretnie w przepisie prawa powszechnie obowiązującego.

Uwzględnienie powyższych wskazówek, przekazanych jako eksperckie wsparcie, niewątpliwie przyczyni się do właściwego wdrożenia zasad ochrony danych wynikających z przepisów rozporządzenia 2016/679 w procedowanych aktach normatywnych z zakresu zmian deregulacyjnych.

[8] M. in. w art. 22^{1b} § 3 Kodeksu pracy, art. 93b ust. 4 ustawy Prawo spółdzielcze, art. 36 ust. 4 ustawy o badaniach klinicznych produktów leczniczych stosowanych u ludzi, art. 27 ust. 2 ustawy o ochronie sygnalistów, art. 42 ust. 14 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi czy art. 13b ust. 11 ustawy o drogach publicznych.

Jednocześnie dziękuję uprzejmie Panu Ministrowi za przedstawienie rozważanych zmian prawnych do zaopiniowania przez Prezesa Urzędu Ochrony Danych Osobowych.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych