

Magdalena Kot
Lawmore
magdalena.kot@lawmore.pl

Bezpieczne przetwarzanie danych wrażliwych

Słowa kluczowe: dane wrażliwe, dane osobowe, RODO

Rozporządzenie PE 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 (dalej RODO) ma skuteczniej chronić dane wrażliwe.

Zasady przetwarzania

RODO wprowadza wiele zmian w przedmiocie przetwarzania danych wrażliwych tzw. danych sensytywnych, czyli danych dotyczących kluczowych obszarów wolności i prywatności osób fizycznych, które od 25 maja 2018 r. będą określane terminem „dane szczególne”.

Według nowych przepisów za dane wrażliwe będą uznawane informacje ujawniające pochodzenie rasowe, etniczne, przekonania polityczne i światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dotyczące stanu zdrowia, seksualności oraz orientacji seksualnej jednostek. Przy czym w przypadku danych biometrycznych RODO wprowadza możliwość ustalenia przez państwa członkowskie indywidualnych zasad przetwarzania danych genetycznych, biometrycznych oraz dotyczących stanu zdrowia w sytuacji ich przetwarzania na dużą skalę i w interesie publicznym. Warto podkreślić, że niektóre kategorie danych osobowych uznane obecnie za wrażliwe w nowym porządku prawnym nie będą uznawane za dane szczególne. Dotyczy to informacji o przekonaniach filozoficznych, przynależności wyznaniowej, przynależności partyjnej, wyrokach skazujących, orzeczeniach o ukaraniu i mandatach karnych, innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym oraz nałogach.

RODO wprowadza generalny zakaz przetwarzania danych sensytywnych, który nie będzie obowiązywał w przypadku spełnienia określonych warunków. Nie należy do nich uzasadniony interes administratora. Przetwarzanie danych sensytywnych stanowi zatem wyjątek od generalnego zakazu ich przetwarzania.

Pierwszą z przesłanek dla legalnego przetwarzania danych wrażliwych będzie udzielenie przez uprawnionego wyraźnej, jednoznacznej, dobrowolnej i świadomie podjętej odnośnie celów, konsekwencji przetwarzania i podmiotu przetwarzającego, zgody na przetwarzanie. Udzielić jej będzie można w dowolnej formie, także pisemnej.

Dopuszczalne będzie również przetwarzanie danych sensytywnych w celu wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, ale tylko gdy takie działania zostały przewidziane przez przepisy unijne lub regulacje krajowe państw członkowskich, lub wynikają z porozumień gwarantujących odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą. A także w sytuacji, gdy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody. Jednak udzielenie zgody nie będzie skuteczne, jeśli jest to niedozwolone prawem Unii Europejskiej lub prawem państwa członkowskiego.

Możliwe będzie także przetwarzanie danych wrażliwych osoby, która uprzednio je upubliczniła, a także wówczas, gdy przetwarzanie takie stało się niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy. Podobnie w sytuacji, kiedy przetwarzanie jest konieczne ze względów związanych z istotnym interesem publicznym, na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu i nie naruszają istoty prawa do ochrony danych oraz gwarantują odpowiednie i konkretne środki ochrony praw podstawowych i interesów uprawnionego.

RODO zezwala także na przetwarzanie danych szczególnych w związku z realizacją profilaktyki zdrowotnej lub medycyny pracy, w tym w szczególności w sytuacji dokonywania oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego, jak też w oparciu o zawartą umowę z pracownikiem służby zdrowia i zastrzeżeniem warunków zabezpieczeń. Prawo unijne dopuszcza także działanie na danych wrażliwych w sytuacji, gdy jest to związane z czynnościami prewencyjnymi z zakresu zdrowia publicznego przed potencjalnymi transgranicznymi zagrożeniami zdrowotnymi. Również uzasadnieniem dla przetwarzania danych sensytywnych jest zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, wynikających ze standardów UE lub państw członkowskich.

Ponadto przetwarzanie danych szczególnych będzie możliwe w interesie publicznym dla prowadzenia badań naukowych, historycznych lub do celów statystycznych. W tym przypadku stosowanie przesłanki niezbędności do wykonania zadania realizowanego w interesie publicznym powinno być ograniczone do administratorów z sektora publicznego, sprawujących powierzoną im władzę publiczną lub działania publiczne. W takiej sytuacji warunkiem dopuszczalności przetwarzania będzie niezbędność przetwarzania danych do wykonywania zadania w interesie publicznym lub sprawowania władzy publicznej.

Warunki specjalne

RODO nakłada na administratorów przetwarzających dane wrażliwe obowiązek wprowadzenia wyższych standardów w zakresie bezpieczeństwa przetwarzania danych. Przejawia się to m.in. w konieczności powołania inspektora ochrony danych osobowych, tj. podmiotu wspierającego administratorów w zachowaniu wymagań określonych przez RODO w zakresie bezpieczeństwa przetwarzania danych osobowych. Obowiązek jego powołania spoczywa na administratorach dokonujących regularnego i systematycznego monitorowania osób, na dużą skalę, a także, gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu szczególnych kategorii danych osobowych.

RODO wymaga też, aby administratorzy dokonujący kompleksowej oceny czynników osobowych osób fizycznych, na podstawie profilowania tych danych lub po przetworzeniu szczególnych kategorii danych osobowych, danych biometrycznych lub danych osobowych dotyczących wyroków skazujących, naruszeń prawa lub innych tego rodzaju orzeczeń, przeprowadzali uprzednią ocenę skutków przetwarzania (dalej OSP), będącą szczegółową analizą przewidywanych konsekwencji, z punktu widzenia bezpieczeństwa danych osobowych, wprowadzenia przez administratora nowych rozwiązań technologicznych lub organizacyjnych. W ramach OSP administrator będzie zobowiązany do opracowania planu działań zabezpieczających dane, które będą przetwarzane oraz określenia, jaki będzie cel przetwarzania. Dodatkowo przetwarzający będzie zobligowany do wskazania, jakie prawnie uzasadnione interesy będą realizowane w związku z przetwarzaniem oraz czy operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów.

W OSP sporządzanej przez administratora muszą się także znaleźć opinie podmiotów zewnętrznych odnośnie ryzyka naruszenia praw lub wolności osób, których dane dotyczą w związku z planowanym przez niego przetwarzaniem oraz informacje odnośnie tego, jakie środki zapobiegawcze miałyby być podejmowane w sytuacji zaistnienia ewentualnego zagrożenia bezpieczeństwa przetwarzania. OSP musi też zawierać opis planowanych do wprowadzenia mechanizmów bezpieczeństwa zwiększających ochronę danych osobowych.

Dokonując oceny skutków przetwarzania danych wrażliwych administratorzy winni się posilkować z jednej strony ustaleniami zawartymi w treści zatwierdzonych już kodeksów postępowania branżowych, a z drugiej stanowiskiem wyrażonym przez przedstawicieli osób, których dane miałyby być przetwarzane.

Dane wrażliwe a nauka

Przetwarzanie danych wrażliwych w celach naukowych i badawczych w interesie publicznym stanowi specyficzny rodzaj przetwarzania danych i winno być szeroko interpretowane. W przypadku badań naukowych będą to działania związane z rozwojem technologicznym w zakresie wprowadzenia prototypowych rozwiązań zarówno w fazie testów, prac eksperymentalnych oraz badań stosowanych. Dotyczy to prac podejmowanych zarówno ze środków publicznych, jak i środków prywatnych, w tym także w ramach europejskiej przestrzeni badawczej, utworzonej w oparciu o art. 179 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.U.2004.90.864/2).

Przykładowymi obszarami obejmującymi europejską przestrzeń badawczą są działania związane z pracami wprowadzającymi nowatorskie rozwiązania w sferze zapobiegania problemom zdrowotnym w przestrzeni publicznej, np. takich jak schizofrenia czy grypa albo rak, w tym w szczególności rozpropagowywania wyników badań naukowych oraz prowadzenia ich na większej liczbie uczestników, w oparciu o szersze połączenie i analizę czynników społecznych.

Z kolei zgodnie z motywem 160 RODO badania naukowe historyczne i genealogiczne, z wyłączeniem danych osób zmarłych (także w celach archiwalnych), w zakresie przetwarzania danych wrażliwych w celach publicznych mają obejmować te zagadnienia, prowadzące do przekazywania danych odnośnie systemów politycznych, w tym państw totalitarnych, o przypadkach ludobójstwa, zbrodniach przeciwko ludzkości (zwłaszcza holokaucie) i zbrodniach wojennych. RODO dopuszcza także przetwarzanie danych wrażliwych w celu realizacji celu publicznego, którym może być także przetwarzanie danych osobowych do badań statystycznych lub opracowywanie wyników statystycznych, które mogą służyć do dalszych celów, m.in. do badań naukowych.

Publiczne przetwarzanie danych wrażliwych

Przetwarzanie wrażliwych danych osobowych w interesie publicznym łączy się z koniecznością wprowadzenia przez administratorów odpowiednich zabezpieczeń celem zagwarantowania odpowiednich praw i wolności osoby, której dane dotyczą. Zgodnie z RODO obowiązek ten może być zrealizowany poprzez wdrożenie środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji przetwarzania danych np. w postaci zastosowania pseudonimizacji lub szyfrowania danych. Administrator musi też stale monitorować, na ile przetwarzanie danych osobowych jest konieczne do osiągnięcia celu. Szczegółowe warunki przetwarzania

danych wrażliwych w interesie publicznym mogą być doprecyzowane indywidualnie w krajowych porządkach prawnych państw członkowskich. Dotyczy to także warunków, w jakich (co dopuszcza RODO) możliwe będzie w ramach przetwarzania danych wrażliwych w interesie publicznym dla celów naukowych, ograniczenie lub wyłączenia praw podmiotów, których dane będą przetwarzane poczynając od prawa do indywidualnej kontroli, prawa dostępu do danych, prawa do sprostowania danych, prawa do ograniczenia przetwarzania oraz prawa do wniesienia sprzeciwu w zakresie dalszego przetwarzania czy prawa do informacji. W przypadku administratorów, którzy uzyskali dane w sposób inny niż od osoby, której one dotyczą, istnieje generalny obowiązek informacyjny. Nie będzie on miał jednak zastosowania, jeśli przekazanie informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku (art. 14 ust. 5 RODO) lub gdyby mogło poważnie utrudnić realizację celów badań naukowych. Dla oceny, czy spełnienie obowiązku informacyjnego jest konieczne, decydująca powinna być liczba osób, których dane dotyczą, okres przechowywania danych oraz zastosowane zabezpieczenia (motyw 62 RODO). Ponadto zgodnie z pkt 159 Preambuły RODO, jeżeli wynik badań naukowych, w szczególności w kontekście zdrowotnym, uzasadnia wprowadzenie dalszych środków w interesie osoby, której dane dotyczą, do środków tych powinny mieć zastosowanie przepisy rozporządzenia. Zgoda w tym zakresie, udzielona przez uprawnionego zgodnie z wymaganiami RODO, uprawnia do publikacji danych osobowych zarówno zwykłych, jak i wrażliwych.

Jakie zmiany

Największe zmiany wprowadzone przez RODO w zakresie przetwarzania szczególnych kategorii danych osobowych obejmują wprowadzenie nowego pojęcia „szczególnych kategorii danych osobowych” zamiast dotychczas funkcjonującego w polskiej literaturze pojęcia „danych wrażliwych”. Nowe przepisy uchylają wyrażanie zgody na przetwarzanie danych szczególnych w innej niż pisemnej formie. Dodatkowo katalog danych został wzbogacony o nową kategorię – dane biometryczne. Nowością jest także obowiązek powoływania Inspektora Ochrony Danych w sytuacji przetwarzania danych wrażliwych na dużą skalę oraz konieczność przeprowadzania OSP, także, gdy planowane jest przetwarzanie danych wrażliwych lub ewentualnie mogłoby dojść do ich naruszenia.