Warszawa, 27.06.2023 r.

Rejestr czynności przetwarzania danych osobowych – w jaki sposób go prowadzić?

Rejestr czynności przetwarzania (RCP) to podstawowe narzędzie wspierające administratorów, pozwalające usystematyzować wykonywane czynności przetwarzania danych osobowych i pomagające wykazać przestrzeganie zasady rozliczalności.

Jaki jest cel prowadzenia rejestru?

Motyw 82 RODO określa dwie podstawowe funkcje obowiązku prowadzenia rejestru:

- zachowanie przez administratora zgodności z RODO;
- umożliwienie organowi nadzorczemu monitorowania prowadzonego przetwarzania.

Prowadzony przez administratorów RCP pozwala im usystematyzować wykonywane czynności oraz całościowo spojrzeć na wykonywane operacje przetwarzania danych osobowych pod względem zgodności zarówno z celami biznesowymi, jak i wymaganiami prawnymi.

Wykonywanie obowiązku określonego w art. 30 RODO pozwala także na stałą weryfikację swojej działalności w zakresie przetwarzania danych osobowych oraz poddawanie ocenie każdego nowo wprowadzanego lub modyfikowanego procesu już na jego najwcześniejszym etapie.

Co zawiera RCP?

Elementy, z których składa się rejestr dzielimy na obligatoryjne i fakultatywne. Obligatoryjne elementy RCP zawarte zostały w art. 30 ust. 1 RODO:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora, oraz wszelkich współadministratorów;
- dane przedstawiciela administratora oraz inspektora ochrony danych;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- informację o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń - gdy ma to zastosowanie,
- jeżeli jest to możliwe - planowane terminy usunięcia poszczególnych kategorii danych;
- jeżeli jest to możliwe - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Brak któregoś z wymienionych powyżej elementów oznacza, że rejestr nie jest kompletny, a tym samym – jest prowadzony z naruszeniem art. 30 ust. 1 RODO.

Kto jest zobowiązany do prowadzenia RCP?

Obowiązek prowadzenia rejestru czynności spoczywa na administratorze, czyli osobie fizycznej lub prawnej, organie publicznym, jednostce lub innym podmiocie, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Zgodnie z art. 30 ust. 5 RODO, obowiązek prowadzania RCP nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że czynności przetwarzania, które wykonują: 1) mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, 2) nie mają charakteru sporadycznego lub obejmują szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub 3) dotyczą wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Jak należy rozumieć pojęcie „czynności przetwarzania"?

RODO nie definiuje pojęcia „czynności przetwarzania", jednak posługuje się nim w kilku przepisach lub motywach w różnych kontekstach, np.:

- „Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach." (motyw 32),
- „Aby stwierdzić, czy czynność przetwarzania można uznać za monitorowanie zachowania osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w Internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw." (motyw 24).

Natomiast samo pojęcie „przetwarzanie" zostało zdefiniowane w art. 4 pkt 2 RODO jako *operacja lub zestaw operacji na danych, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie*. Powstaje zatem pytanie, jak należy interpretować pojęcie „czynności przetwarzania danych", biorąc pod uwagę ww. definicję oraz fakt, że rejestr takich czynności odnosi się nie tylko do pojedynczych czynności przetwarzania, ale, jak wynika również z angielskiej wersji dokumentu („records of procesing activities") do czynności w liczbie mnogiej.

Analizując motywy i przepisy w kontekście obowiązku określonego w art. 30 ust. 1 RODO, należy przyjąć, że czynności przetwarzania to *zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.*

Czy rejestr może zawierać więcej informacji niż te określone w art. 30?

Wskazane w art. 30 ust. 1 RODO składniki są obligatoryjne. Jednak wskazany w tym przepisie zakres informacji o operacjach wykonywanych w ramach danej czynności nie ma charakteru zamkniętego. Zatem mogą się w nim znaleźć inne elementy, które administrator uzna za zasadne, uwzględniając wiele specyficznych dla niego czynników, takich jak np.:

- wskazanie podstawy prawnej przetwarzania,

- wskazanie źródła pozyskania danych,
- wskazanie użytego do przetwarzania systemu informatycznego,
- informacje dotyczące przeprowadzonej oceny skutków dla ochrony danych itp.,
- określenie tzw. właścicieli procesów, czyli osób odpowiedzialnych u administratora za konkretne czynności przetwarzania (np. kierownik określonej komórki w organizacji, wydzielone stanowisko itp.),
- dane kontaktowe podmiotu przetwarzającego oraz podmiotów, którym podpowierzono wykonywanie określonych czynności przetwarzania danych lub określonych operacji w ramach tych czynności (art. 28 ust. 4 RODO)

Rejestr może zawierać więc więcej informacji niż te wskazane w art. 30 ust. 1 RODO, tak aby kompleksowo objąć procesy przetwarzania danych i zapewnić ich pełną czytelność i transparentność.

W jakiej formie należy prowadzić RCP?

Nie ma jednolitych wytycznych co do formy, układu, wyglądu rejestru. RODO pozostawia dużą dowolność administratorom danych. Stanowi jedynie, że rejestr powinien być prowadzone w formie pisemnej (art. 30 ust. 3), może to być postać zarówno papierowa, jak i elektroniczna. Wielu administratorów korzysta z wersji tabelarycznej rejestru, która została opublikowana przez UODO, jako wzorcowa.

Podsumowanie

Rejestr czynności przetwarzania jest świetnym narzędziem do kontroli procesów wykonywanych na danych osobowych. Rzetelne prowadzenie RCP pozwala administratorowi wykazać przestrzeganie zasady rozliczalności, ale przede wszystkim uporządkować procesy przetwarzania danych osobowych. Należy pamiętać również o tym, że rejestr musi także zostać udostępniony na żądanie organu nadzoru, a kontrole UODO często też zaczynają się od weryfikacji konkretnych procesów w RCP.

Nina Zacharska - specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.