WDROŻENIE RODO

Etapy procesu wdrażania RODO w organizacji

1. Identyfikacja procesów przetwarzania danych osobowych

RODO odchodzi od podejścia opartego o kategorię zbiorów danych, do którego przyzwyczaiła nas ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, na rzecz podejścia opartego o procesy przetwarzania danych osobowych. W pewnym uproszczeniu, proces przetwarzania danych osobowych można opisać jako ciąg następujących po sobie czynności począwszy od zebrania danych osobowych, aż do ich usunięcia. Z tego względu, punktem wyjścia dla wdrożenia RODO w organizacji powinna być identyfikacja istniejących procesów przetwarzania danych.

Przykłady:

• w każdej organizacji – proces przetwarzania danych kadrowo – płacowych,

• w sklepie internetowym – proces przetwarzania danych związanych z transakcjami sprzedaży,

• w podmiocie zajmującym się niszczeniem danych – proces przetwarzania danych niszczonych na zlecenie klientów.

Należy także zidentyfikować te procesy, w których dochodzi do powierzenia przetwarzania danych osobowych:

a) w których podmiot wdrażający RODO jest administratorem powierzającym przetwarzanie

Przykłady:

• powierzenie przez przedsiębiorcę zewnętrznemu podmiotowi prowadzenia księgowości,

• powierzenie przez przedsiębiorcę zewnętrznemu podmiotowi obsługi kadrowo – płacowej

b) w których podmiot wdrażający RODO jest podmiotem przetwarzającym dane na zlecenie administratora.

Przykłady:

• świadczenie przez przedsiębiorcę usług archiwizacji danych osobowych,

• świadczenie przez przedsiębiorcę usług księgowych

Każdy proces przetwarzania danych osobowych powinien zostać opisany przy użyciu jak największej ilości zmiennych, aby w możliwie dokładny sposób oddać jego specyfikę.

2. Weryfikacja podstawowych parametrów procesów przetwarzania danych

Dla każdego zidentyfikowanego procesu przetwarzania danych należy co najmniej:

• określić podstawę przetwarzania danych osobowych zgodną z RODO,

• zweryfikować zakres przetwarzanych danych, zgodnie z zasadą minimalizacji,

• zweryfikować treść obowiązków informacyjnych towarzyszących gromadzeniu danych.

W przypadku, gdy przetwarzanie danych opiera się o

zgody zebrane przed 25 maja 2018 r. należy zweryfikować, czy takie zgody pozostaną nadal ważne. W

tym celu należy ocenić, czy zgody odpowiadają wymogom sformułowanym przez RODO w stosunku do zgody na przetwarzanie danych.

Materiały – Stanowisko GIODO dotyczące ważności zgód na przetwarzanie danych osobowych,

http://giodo.gov.pl/pl/1520281/10303

3. Wdrożenie podejścia opartego na ryzyku

Dla wszystkich procesów przetwarzania danych osobowych należy określić poziom ryzyka związanego z przetwarzaniem danych osobowych i wdrożyć odpowiednie środki zabezpieczenia danych.

Podejście oparte na ryzyku wymaga ciągłego monitorowania poziomu ryzyka związanego z przetwarzaniem danych osobowych. Nie jest więc wystarczającym jednorazowe dla danego procesu określenie poziomu ryzyka i zastosowanie środków zabezpieczenia danych – poziom ryzyka powinien być monitorowany ciągle w ramach trwających procesów przetwarzania danych.

Materiały – Jak rozumieć i stosować podejście oparte na ryzyku? – poradnik GIODO,

http://www.giodo.gov.pl/pl/1520282/10294

4. Przeprowadzenie procedury oceny skutków dla ochrony danych

Wykonanie oceny skutków dla ochrony danych osobowych może być obowiązkowe wyłącznie dla procesów przetwarzania danych, które rozpoczynają się po 25 maja 2018 r. Natomiast dla tych procesów, które w dniu rozpoczęcia stosowania RODO są w toku, przeprowadzenie oceny co do zasady nie jest obowiązkowe. Jeżeli jednak zmieni się poziom ryzyka związanego z przetwarzaniem danych w procesach będących w toku, wówczas przeprowadzenie oceny może stać się obowiązkowe na zasadach ogólnych. Dlatego rekomenduje się przeprowadzenie – w miarę możliwości – oceny skutków dla ochrony danych także dla procesów, które w dniu 25 maja 2018 r. są już w toku.

5. Powierzenie przetwarzania danych

Prawidłowe wdrożenie RODO wymaga zidentyfikowania tych wszystkich procesów przetwarzania danych, w których dochodzi do powierzenia przetwarzania danych.

RODO, w odróżnieniu od ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, nakłada na administratora danych prawny obowiązek wyboru takiego podmiotu przetwarzającego, który zapewnia przestrzeganie RODO. Stąd w sytuacji, gdy podmiot wdrażający RODO jest administratorem powierzającym przetwarzanie danych, powinien on dla każdego podmiotu przetwarzającego dokonać sprawdzenia przestrzegania przez niego postanowień RODO i gotowości do wdrożenia RODO. Jeżeli natomiast podmiot wdrażający RODO jest podmiotem przetwarzającym dane na zlecenie administratora, wówczas powinien on być gotowy na takie sprawdzenia ze strony administratora danych.

Niezależnie od kwestii wyboru podmiotu przetwarzającego, każda umowa powierzenia powinna zostać dostosowana do nowych wymagań treściowych określonych w RODO.

6. Nowe prawa osób, których dane dotyczą

Należy wdrożyć rozwiązania umożliwiające wykonywanie nowych praw osób, których dane dotyczą, na czele z prawem do bycia zapomnianym i prawem do przenoszenia danych. Czasem może to wymagać wprowadzenia zmian w systemach informatycznych, przy współpracy z podmiotami dostarczającymi te systemy – należy więc upewnić się, że takie zmiany zostaną wprowadzone.

7. Incydenty bezpieczeństwa

Należy wdrożyć rozwiązania umożliwiające wykonywanie obowiązku zgłaszania incydentów bezpieczeństwa danych osobowych.

Źródło: „Przewodnik po RODO dla Małych i Średnich Przedsiębiorców” MINISTERSTWO PRZEDSIĘBIORCZOŚCI I TECHNOLOGII Autor dr Paweł Litwiński 2018 r. Warszawa

www.biznes.gov.pl