Warszawa 24.01.2022 r.

Współpraca z procesorem w praktyce – kilka ważnych kwestii

W dzisiejszym artykule nie będziemy skupiać się na samym pojęciu procesora oraz kwestiach związanych z trudnościami w ustaleniu, czy dany podmiot jest procesorem, czy też nie. Skupimy się natomiast na opisaniu etapów, jakie wiążą się ze współpracą z procesorami oraz przydatnej w tej współpracy dokumentacji.

Wybieramy procesora (podmiot przetwarzający)

Zgodnie z RODO powierzając dane osobowe powinniśmy korzystać wyłączenie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Kluczową kwestią z punktu widzenia administratora, czy też szerzej podmiotu, który chce powierzyć dane osobowe do przetwarzania innemu podmiotowi jest sprawdzenie, czy ten podmiot zapewnia te wystarczające gwarancje o jakich mowa w RODO. Pamiętajmy, że to nas, jako podmiot powierzający dane obciąża odpowiedzialność za dokonanie odpowiedniego wyboru. Co powinniśmy uwzględnić szukając odpowiedniego procesora?

Odpowiedni procesor powinien w szczególności:

- posiadać odpowiednią wiedzę fachową i doświadczenie umożliwiającą realizację zleconych zadań;
- posiadać odpowiednie zasoby umożliwiające utrzymanie zdolności do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i procesów przetwarzania;
- posiadać wdrożone odpowiednie środki techniczne i organizacyjne, zgodnie z wymaganiami wskazanymi w art. 32 RODO;
- posiadać wdrożone odpowiednie środki techniczne i organizacyjne umożliwiające pomoc administratorowi danych w realizacji jego obowiązków wynikających z RODO, takich jak np. udzielanie odpowiedzi na żądania osób, których dane dotyczą, zgłaszanie naruszeń;
- umożliwiać przeprowadzenie audytów lub inspekcji;
- gwarantować ciągłą współpracę w zakresie powierzonych danych osobowych poprzez bieżący kontakt, udostępnianie informacji, udzielanie wyjaśnień stosownie do charakteru i zakresu świadczonych usług.

Należy jednak pamiętać, że to tylko kilka najważniejszych kwestii na jakie należy zwrócić uwagę. Z kontekstu dokonywanego powierzenia (z uwagi np. na jego przedmiot, zakres, charakter) mogą wynikać także inne elementy, których powinniśmy wymagać od procesora. W przypadku korzystania przez procesora z innych podmiotów przetwarzających, konieczne będzie zweryfikowanie, czy procesor przestrzega warunków korzystania z innego podmiotu przetwarzającego stawianych przez RODO.

W jaki sposób możemy dokonać sprawdzenia, czy procesor spełnia stawiane mu warunki i zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO? Jedną z możliwości jest wprowadzenie kwestionariusza weryfikacyjnego zawierającego odpowiednie pytania pozwalające na zweryfikowanie, czy potencjalny procesor spełnia wymogi RODO. Kwestionariusz powinien umożliwić zebranie takich informacji, które pozwolą na ocenę, czy procesor wdrożył środki techniczne i organizacyjne odpowiadające kontekstowi przetwarzania i zidentyfikowanemu ryzyku naruszenia praw lub wolności osób fizycznych. Kwestionariusz powinien pozwolić na ocenę, czy dany procesor spełnia także nasze minimalne wymagania jakich oczekujemy w danym przypadku od podmiotu przetwarzającego powierzane przez nas dane, jeśli ustaliliśmy takie minimalne wymagania dla konkretnego procesu przetwarzania oraz czy będzie z nami

współpracował w czasie powierzenia w oczekiwany przez nas sposób, udzielając nam niezbędnych informacji, w odpowiednim czasie informując o zaistniałych naruszeniach czy innych problemach.
Przykładowe elementy kwestionariusza:

- weryfikacja miejsca przetwarzania danych;
- pytania dotyczące ilości zatrudnianych osób/ możliwości personalnych wykonania usługi/ zatrudniania wystarczającej liczby osób dla zapewnienia ciągłości przetwarzania danych;
- weryfikacja powołania IOD przez potencjalnego procesora;
- pytania dotyczące szkoleń pracowników w zakresie ochrony danych osobowych, polityki upoważnień pracowników do przetwarzania danych, obowiązku zachowania poufności;
- pytania dotyczące ustalenia i wdrożenia polityk ochrony danych osobowych, procedur związanych z ochroną danych osobowych, posiadanych certyfikatów związanych z ochroną danych osobowych;
- pytania dotyczące spełniania obowiązków nałożonych na procesora bezpośrednio przez RODO np. prowadzenia rejestru kategorii czynności przetwarzania, dokonywanie regularnego przeglądu stosowanych środków organizacyjnych i technicznych;
- pytania pozwalające sprawdzić, czy procesor stosuje odpowiednie środki techniczne i organizacyjne, by pomóc nam w odpowiadaniu na żądania osób których dane dotyczą, np. posiada procedurę zgłaszania naruszeń, ma możliwość przekazania nam żądań osób, których dane dotyczą w odpowiednim terminie oraz udzielenia nam odpowiedzi związanych z przetwarzaniem danych dokonywanym przez procesora;
- pytania pozwalające sprawdzić czy i jakie systemy informatyczne procesor będzie wykorzystywał do przetwarzania danych;
- pytania pozwalające sprawdzić jakie środki techniczne zastosował procesor;
- pytania pozwalające sprawdzić, czy procesor przy realizacji naszej usługi będzie korzystał z innych podmiotów przetwarzających;
- pytania pozwalające sprawdzić, czy procesor przy realizacji naszej usługi będzie przekazywał dane osobowe poza obszar EOG.

I jeszcze jedna ważna kwestia. Takiej oceny powinniśmy dokonywać zawsze na etapie wyboru odpowiedniego podmiotu, a więc zanim jeszcze podpiszemy umowę, rozpoczniemy współpracę. Może się bowiem okazać, że podmiot, który wstępnie wybraliśmy (bo np. oferuje korzystne warunki współpracy) nie spełnia ostatecznie wymogów stawianych przez RODO i nie daje wystarczających gwarancji na zgodne z RODO przetwarzanie powierzonych przez nas danych. Z punktu widzenia ochrony danych osobowych nie powinniśmy z takim podmiotem podejmować współpracy i powierzać mu do przetwarzania danych osobowych. Powierzenia do przetwarzania danych osobowych takiemu podmiotowi sprawia, że to my nie spełniamy wymagań stawianych nam w tym przypadku przez RODO, a więc nie wybraliśmy odpowiedniego procesora.

Powierzamy do przetwarzania dane osobowe

Powierzając do przetwarzania dane osobowe zawieramy umowę powierzenia. Powinna ona zawierać elementy wskazane w art. 28 RODO. Z punktu widzenia praktycznej strony naszej współpracy z procesorem ważnym elementem umowy będzie określenie praw administratora. Musimy pamiętać, że mimo powierzenia do przetwarzania danych innemu podmiotowi, to nadal my, jako podmiot powierzający jesteśmy zobowiązani do wykonywania obowiązków nałożonych na nas przez RODO, np. odpowiedzi na żądania podmiotów danych, współpraca z organem, zgłaszanie naruszeń danych osobowych, spełnienie obowiązku informacyjnego.
W przypadku powierzenia przetwarzania danych osobowych wiele informacji niezbędnych do wykonania tych obowiązków znajdować się będzie w posiadaniu procesora. W związku z tym z punktu widzenia

podmiotu powierzającego dane do przetwarzania, musimy zadbać, by otrzymywać niezbędne nam do wypełnienia obowiązków wynikających z RODO informacje w odpowiednim czasie i formie, a więc tak doprecyzować elementy wskazane w art. 28 RODO, byśmy mogli bez przeszkód wypełniać nasze obowiązki. Warto więc doprecyzować terminy jakie będzie miał procesor na przekazanie nam informacji, np. o tym, że miało miejsce naruszenie, że osoba, której dane dotyczą zgłosiła żądanie dostępu do danych osobowych.
Może się także okazać, że część obowiązków będzie za nas wykonywał procesor, np. spełniał obowiązek informacyjny w związku z tym, że to on w naszym imieniu będzie pierwszy kontaktował się osobami, których dane dotyczą. W takim wypadku musimy zadbać, by procesor otrzymał od nas zarówno niezbędne treści, jak i wskazówki co do wypełnienia tych obowiązków.

Monitorowanie współpracy z procesorem

Sam wybór procesora i podpisanie z nim umowy powierzenia nie kończy obowiązków jakie wynikają z faktu powierzenia przetwarzania danych osobowych innemu podmiotowi. Jako podmiot powierzający do przetwarzania dane osobowe zobowiązani jesteśmy co stałego monitorowania współpracy z procesorem, badania, czy sytuacja nie uległa zmianie, czy nadal spełnia on dotychczasowe warunki, bądź czy procesor nadal zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych aby przetwarzanie spełniało wymogi RODO.
Odpowiedzialność za wybór odpowiedniego procesora rozciąga się na czas całej z nim współpracy w zakresie powierzenia do przetwarzania danych. Samo RODO daje nam w tym zakresie uprawnienie do żądania od procesora informacji, które są niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz do przeprowadzenia audytów lub inspekcji u procesora. Warto w tym zakresie ustalić wewnętrzne zasady przeprowadzania sprawdzenia procesorów, biorąc pod uwagę to jakie procesy przetwarzania przekazujemy podmiotom zewnętrznym, jakie dane powierzamy, jak długo będzie trwała współpraca, z jakimi zagrożeniami może się wiązać. W takich zasadach możemy ustalić:

- narzędzia służące nam do weryfikacji procesora w toku współpracy (kwestionariusz weryfikacyjny, audyt, inspekcja, okresowe przekazywanie informacji);
- częstotliwość/ terminy dokonywania sprawdzeń;
- warunki wykorzystania poszczególnych narzędzi (kiedy wykorzystujemy jakie narzędzie);
- warunki przeprowadzenia audytu/ inspekcji;
- sposób dokumentowania dokonywanej weryfikacji.

Ustalony sposób weryfikowania procesora w toku współpracy warto doprecyzować w umowie powierzenia, określić częstotliwość, zasady ich przeprowadzania oraz czas trwania. Tak ustalone zasady mogą stanowić element procedury współpracy z procesorami.

Procedura współpracy z procesorami (podmiotami przetwarzającymi)

Kwestie współpracy z procesorami warto uregulować w jednym dokumencie wchodzącym w skład polityki ochrony danych osobowych. Taka procedura w sposób kompleksowy uporządkuje kwestie wyboru procesora, zawierania umowy powierzenia, monitorowania współpracy z procesorem oraz wskaże osoby odpowiedzialne za poszczególne elementy współpracy. Procedura taka może zawierać:

- zasady zarządzania usługami wykonywanymi przez procesora;
- wskazanie osób odpowiedzialnych za poszczególne czynności/ obszary współpracy;
- zasady powierzania przetwarzania danych osobowych, w tym wzór umowy powierzenia;
- sposób wyłaniania procesora, określania minimalnych wymagań w zakresie bezpieczeństwa (technicznych i proceduralnych) przetwarzania jakie powinien spełniać, w tym określenie wzoru modelowego kwestionariusza weryfikacyjnego;

- określenie roli i zadań IOD w procesie powierzania przetwarzania danych osobowych;
- zasady, sposób, osoby odpowiedzialne za monitorowanie współpracy z procesorem;
- zasady, terminy i sposób przeprowadzania audytów/inspekcji u procesorów lub innych sposobów weryfikacji procesorów w toku współpracy.

Są to przykładowe elementy jakie mogą podlegać regulacji w procedurze współpracy z procesorem. W zależności od potrzeb można wprowadzać dodatkowe elementy. Przykładowo w przypadku korzystania z dużej liczby procesorów przydatny może być rejestr umów powierzenia, gdzie w jednym miejscu zostaną zgromadzone najważniejsze informacje z umów, ułatwiający zarządzanie nimi i powierzonymi danymi. W przypadku przekazywania regularnie dużej ilości danych, procedura taka może przewidywać zasady ich przekazywania/ zabezpieczania.

Zakończenie współpracy z procesorem

W przypadku zakończenia współpracy z procesorem zgodnie z RODO zobowiązany jest on do usunięcia lub zwrotu danych osobowych (zależnie od wyboru administratora) oraz usunięcia ich wszystkich kopii. Czynności te, z uwagi na zasadę rozliczalności, powinny być udokumentowane np. protokołem z ich przeprowadzenia. Dokument potwierdzający dokonanie wyżej wskazanych czynności powinien zawierać informacje o tym kto, kiedy, na jakiej podstawie i w jaki sposób dokonał określonych czynności (zniszczenia lub zwrotu danych). Dokument taki powinniśmy przechowywać jako dowód spełnienia przez procesora jego obowiązków związanych z zakończeniem powierzenia przetwarzania danych osobowych.

Ewa Eluszkiewicz – specjalista ds. Ochrony danych iSecure Sp. o.o.