URZĄD OCHRONY DANYCH OSOBOWYCH

Urząd Zamówień Publicznych

OCENA PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH W ZAMÓWIENIACH PUBLICZNYCH

Monika Krasińska

Dyrektor Departamentu Prawa i Nowych Technologii

Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych
ul. Stanisława Moniuszki 1A, 00-014 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

PODSTAWY PRAWNE

Cele ogólnego rozporządzenia o ochronie danych osobowych

- Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych **(motyw 6 RODO).**
- W zakresie, w jakim niniejsze rozporządzenie dopuszcza doprecyzowanie lub zawężenie jego przepisów przez prawo państw członkowskich, mogą one – o ile jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy niniejszego rozporządzenia do swego prawa krajowego **(motyw 8 RODO)**
- **Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych**

OBOWIĄZKI ADMINISTRATORA

Projektowanie ochrony danych osobowych – art. 25 RODO

- **Realizacja obowiązków związanych z przestrzeganiem przepisów o ochronie danych osobowych w dokumentacji zamówienia – zasada rozliczalności (art. 5 ust. 2 RODO)**
- **dokumenty zamówienia** –dokumenty sporządzone przez zamawiającego lub dokumenty, do których zamawiający odwołuje się, inne niż ogłoszenie, służące do określenia lub opisania warunków zamówienia, w tym specyfikacja warunków zamówienia oraz opis potrzeb i wymagań (art. 7 pkt 3 pzp)
- **identyfikacja danych osobowych i procesów przetwarzania danych osobowych na poszczególnych etapach projektowania zamówienia publicznego** - od zaplanowania postępowania przez przeprowadzenie postępowania aż po udzielenie zamówienia publicznego

OBOWIĄZKI ADMINISTRATORA

Projektowanie ochrony danych osobowych – art. 25 RODO

<u>Przedmiot zamówienia to nie tylko produkt czy usługa ale także powiązane z nimi procesy przetwarzania danych osobowych</u>

Konieczność dokonania przez Zamawiającego:

- **oceny czy zaprojektowane zamówienie respektuje zasady ochrony danych (art. 5 ust. 1 RODO) i wykazania, że jest zgodne z przepisami o ochronie danych osobowych (art. 5 ust. 2 RODO)**
- **analizy ryzyka**
- **oceny skutków dla ochrony danych (przy wystąpieniu warunków z art. 35 RODO)**
- **zgodności z wymogami wynikającymi z odrębnych przepisów prawa (np. przepisami o cyberbezpieczeństwie, przepisami o sztucznej inteligencji, przepisami prawa pracy, przepisami kształtującymi tajemnice prawnie chronione, odrębne tryby dostępowe czy okresy retencji danych)**
- **oceny zgodności z Prawem zamówień publicznych (np. określenie granic jawności i poufności danych – art. 74 ust. 4 czy art. 81 pzp)**

OBOWIĄZKI ADMINISTRATORA

Projektowanie ochrony danych osobowych – art. 25 RODO

- **W wielu przypadkach oceny wymagać będzie także zapewnienie zgodności zamówienia w zakresie przetwarzania danych osobowych z prawami podstawowymi – konieczność przeprowadzenia testu prywatności, określenia adekwatnych i niezbędnych granic ingerencji w autonomię informacyjną jednostki.**

OBOWIĄZKI ADMINISTRATORA

Powierzenie danych osobowych – art. 28 RODO

Zamawiający jako administrator odpowiada za:

- **Identyfikację Wykonawcy jako przetwarzającego (art. 4 pkt 8 RODO)**
- **Dokonanie wyboru przetwarzającego przy spełnieniu kryteriów określonych w RODO** – korzystanie wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby **(motyw 81 RODO)**
- **Przeniesienie obowiązków z art. 28 i 32 RODO do dokumentacji zamówienia tak aby ograniczyć ryzyka dla podmiotów danych, zapewnić kontrolę Wykonawcy jako przetwarzającego i ukształtować przesłanki do ewentualnego rozwiązania umowy**

Przetwarzający ma pomagać administratorowi w wywiązywaniu się z obowiązków wynikających z przepisów o ochronie danych osobowych (art. 28 ust. 3 lit e i f RODO)

OBOWIĄZKI ADMINISTRATORA

Powierzenie danych osobowych

Jak badać podmioty przetwarzające pod kątem spełnienia kryterium „wystarczających gwarancji”?

- **Referencje odnoszące się do wysokiej jakości usługi czy przyjęcie wysokiej oceny reputacji Wykonawcy nie przesądzają o bezpieczeństwie danych ani spełnieniu innych warunków wynikających z art. 28 RODO**
- Konieczność dokonania oceny: środków techniczno-organizacyjnych, zastosowanych technologii, powiązań z innymi podmiotami (podwykonawcami) i ryzyk związanych z przekazywaniem danych do krajów trzecich nie zapewniających odpowiedniego poziomu ochrony danych osobowych, struktury odpowiedzialności, zdolności reagowania na incydenty i naruszenia, zarządzania bezpieczeństwem
- Wystarczające gwarancje podmiot przetwarzający może wykazać między innymi poprzez **stosowanie zatwierdzonego kodeksu postępowania**, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 (art. 28 ust. 3 RODO)

OBOWIĄZKI ADMINISTRATORA

Powierzenie danych osobowych

1. Ocena zakresu wymagań dla przetwarzającego - w jaki sposób ma udokumentować swoją zdolność przetwarzania w myśl reguł ochrony danych osobowych dedykowanych procesorowi, czy poprzez przedłożenie:

- Deklaracji zgodności z RODO i adekwatności przyjętych środków bezpieczeństwa?
- Polityk ochrony danych osobowych?
- Analizy ryzyka? - zgodnie z art. 32 RODO podmiot przetwarzający również ma obowiązek wdrożyć środki bezpieczeństwa adekwatne do ryzyka

Kiedy jej żądać: - przed złożeniem oferty, po przyjęciu oferty ale przed zawarciem umowy czy po zawarciu umowy?

2. Określenie etapu przedłożenia wymagań Zamawiającego – konieczność doboru właściwego trybu postępowania

– stosowanie negocjacji lub dialogu konkurencyjnego w przypadkach uznania ochrony danych osobowych i bezpieczeństwa danych za kluczowe (art. 275 pkt 3 pzp)

OBOWIĄZKI ADMINISTRATORA

Odpowiedzialność administratora

Zamawiający ponosi odpowiedzialność za przetwarzanie danych osobowych i musi być świadomy wszystkich ryzyk na jakie się umawia!

- Ustalenie procedury wyboru i kontroli przetwarzającego oraz egzekwowania postanowień umowy w trakcie jej realizacji
- Przeprowadzenie najpierw własnej analizę ryzyka, która zdefiniuje oczekiwania względem przetwarzającego – to nie przetwarzający decyduje czy ryzko jest niskie czy wysokie
- Oczekiwanie udokumentowania analizy ryzyka przetwarzającego pierwotnego i wtórnie przetwarzających
- Wprowadzenie listy kontrolnej w zakresie spełnienia kluczowych wymogów RODO
- Sprawowanie stałego nadzoru nad realizacją umowy powierzenia także po zakończeniu procedury przetargowej – faktyczna kontrola nad błędami swoimi i swojego przetwarzającego

Szczególna rola opiniodawcza - kontrolna Inspektora Ochrony Danych Osobowych w zamówieniach publicznych – art. 39 RODO

URZĄD OCHRONY DANYCH OSOBOWYCH

Urząd Zamówień Publicznych

DZIĘKUJĘ ZA UWAGĘ

Urząd Ochrony Danych Osobowych
ul. Stanisława Moniuszki 1A, 00-014 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl