|  |  |  |
| --- | --- | --- |
|  | **Procedura powierzenia przetwarzania danych osobowych** Ośrodka Kultury Fizycznej i Rekreacji w Śmiglu | |
| Załącznik do Polityki bezpieczeństwa danych osobowych | |
| Wersja: 01 | Data: 22.10.2024 |
| Opracowane przez: Kierownika OKFiR Śmigiel Zygmunta Ratajczaka | |

W przypadku gdy **administrator** danych osobowych - Ośrodek Kultury Fizycznej i Rekreacji w Śmiglu *(zwany dalej „OKFiR Śmigiel”)* chciałby, aby czynności przetwarzania wykonywał za OKFiR Śmigiel inny podmiot, **administrator może powierzyć przetwarzanie danych**. Wymogi dotyczące powierzenia zostały określone w art. 28 **RODO**[[1]](#footnote-1). Prawodawca unijny nakłada na administratora obowiązek wyboru **podmiotu przetwarzającego**, który zapewni przestrzeganie przepisów RODO. Podstawą powierzenia może być umowa lub inny instrument prawny. Przepis art. 28 ust. 3 RODO określa wymogi co do treści tego rodzaju umowy lub innego instrumentu prawnego. Prawodawca unijny rozstrzygnął również kwestię dalszego powierzenia *(****podpowierzenia****)* **danych** - jest ono dopuszczalne, zgodnie z art. 28 ust. 2 RODO - jeżeli administrator wyrazi na to zgodę. **Podmiot, któremu podmiot przetwarzający na zlecenie administratora powierzył przetwarzanie *(podwykonawca)*, powinien spełniać wymogi, jakie odnoszą się do podmiotu przetwarzającego.** Prawodawca unijny przewidział możliwość wykorzystania w konstrukcji powierzenia przetwarzania zatwierdzonych kodeksów postępowania, zatwierdzonych mechanizmów certyfikacji oraz standardowych klauzul umownych. Jeżeli **podmiot przetwarzający naruszy przepisy RODO przy określaniu celów i sposobów przetwarzania, zgodnie z art. 28 ust. 10 RODO uznaje się go za administratora w odniesieniu do tego przetwarzania.**

1. **Zaistnienie potrzeby powierzenia przetwarzania danych**

**Administrator -** OKFiR Śmigiel może uznać, że nie jest technicznie bądź organizacyjnie przygotowany do dokonywania określonych operacji na danych osobowych w ramach procesów przetwarzania, bądź że inny podmiot jest w stanie wykonać te działania lepiej, taniej bądź szybciej. W tej sytuacji administrator powinien rozważyć możliwość skorzystania z konstrukcji powierzenia przetwarzania danych. Powierzenie może dotyczyć różnego rodzaju czynności przetwarzania danych, *np. zgromadzenie danych, wprowadzenie danych do systemu informatycznego, usunięcie danych itp.* **Zawarcie umowy powierzenia zależeć jednak będzie od tego co zostało zlecone *(jaki jest przedmiot umowy zlecenia).***Jeśli przedmiotem zlecenia jest przetwarzanie danych to wówczas przeprowadzamy analizę podmiotu zewnętrznego, jeżeli wynika z niej konieczność zawarcia tego typu umowy należy pamiętać o przepisach regulujących jej zakres. Kluczowy w tym obszarze jest art. 28 RODO, który wprost wskazuje niezbędne elementy umowy powierzenia przetwarzania danych osobowych. Należy zwrócić uwagę, że **uregulowanie relacji pomiędzy administratorem i podmiotem przetwarzającym w oparciu o umowę powierzenia** lub inny instrument prawny **jest obowiązkiem administratora oraz podmiotu przetwarzającego.** Brak jego spełnienia może być podstawą do nałożenia administracyjnej kary pieniężnej zgodnie z art. 83 ust. 4 lit. a) RODO. **Innym wzorem umowy na powierzenie przetwarzania danych osobowych są standardowe klauzule umowne zatwierdzone przez Komisję Europejską**: Decyzja wykonawcza Komisji *(UE)* 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 RODO oraz art. 29 ust. 7 Rozporządzenia Parlamentu Europejskiego i Rady *(UE)* 2018/1725.

1. **Ocena czy przepisy szczególne regulują kwestie powierzenia przetwarzania danych**

Kwestia powierzenia przetwarzania danych może być przedmiotem regulacji przepisów szczególnych, które mogą potwierdzać dopuszczalność powierzenia przetwarzania, określać bardziej szczegółowe zasady powierzenia albo ograniczać bądź wyłączać możliwość powierzenia przetwarzania danych.

1. **Wybór podmiotu, któremu administrator - OKFiR Śmigiel** **zamierza powierzyć przetwarzanie danych - ocena, czy wybrany podmiot jest w stanie spełnić wymogi RODO.**

Decydując się na powierzenie przetwarzania danych **administrator** powinien dokonać wyboru odpowiedniego podmiotu, któremu powierzy przetwarzanie. Przy dokonywaniu wyboru administrator powinien kierować się nie tylko ceną za świadczone usługi, ale przede wszystkim podstawowym kryterium oceny powinna być możliwość spełnienia przez podmiot przetwarzający wymogów związanych z przetwarzaniem i ochroną danych. **Należy pamiętać, że art. 28 ust. 1 RODO *(uzupełniony treścią motywu 81 RODO),* zobowiązuje administratora, do korzystania jedynie z takich podmiotów przetwarzających, które gwarantują wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających, że przetwarzanie spełnia wymogi RODO oraz chroni prawa osób, których dane są przetwarzane.** W związku z powyższym **administrator powinien przedsięwziąć środki pozwalające mu na** **weryfikację podmiotu przetwarzającego**. Ze względu na bezpieczeństwo danych osobowych i administracyjne kary pieniężne, decyzja administratora w zakresie wyboru podmiotu przetwarzającego nie powinna być podejmowana pochopnie. Przepisy RODO wskazują, że podmiot przetwarzający może wykazać, iż daje wystarczające gwarancje m.in. poprzez stosowanie odpowiedniego zatwierdzonego kodeksu postępowania albo poddał się procesowi certyfikacji i uzyskał stosowny certyfikat. **Kolejną metodą weryfikacyjną, którą może zastosować administrator jest przeprowadzenie audytu podmiotu przetwarzającego lub żądanie wypełnienia formularza - listy kontrolnej pozwalającej na jego sprawdzenie.** Lista kontrolna, ankieta dla podmiotu przetwarzającego *(procesora)* służy weryfikacji podmiotu, któremu administrator planuje powierzyć dane osobowe do przetwarzania, pod kątem stosowanych przez niego środków technicznych i organizacyjnych mających zapewnić zgodność z przepisami RODO. Lista kontrolna zawiera miejsca *(kolumna „odpowiedź”)* w którym podmiot przetwarzający *(procesor)* w sposób skrupulatny ustosunkowuje się do zawartych w dokumencie pytań administratora. Administrator w liście kontrolnej w kolumnie „poziom zgodności” dokonuje oceny poszczególnych środków zapewniających bezpieczeństwo przetwarzania danych według ustalonych kryteriów *(zgodność / częściowa zgodność / niezgodność)* przyjętych w liście kontrolnej, ankiecie dla podmiotu przetwarzającego.

* 1. **Administrator - OKFiR Śmigiel** **przyjął następujące kryteria określające możliwość współpracy z weryfikowanym podmiotem przetwarzającym:**

1. **spełnienie przyjętych kryteriów na poziomie 80% i więcej** - podmiot daje gwarancje wdrożenia odpowiednich środków zapewniających spełnienie wymogów RODO i bezpieczeństwa praw osób, których dane dotyczą - **administrator może rozważyć zawarcie umowy powierzenia przetwarzania danych osobowych;**
2. **spełnienie przyjętych kryteriów na poziomie od 50% do 79%** - podmiot przetwarzający powinien wprowadzić konieczne zmiany w stosowanych środkach technicznych i organizacyjnych według wskazań administratora - **administrator po zweryfikowaniu dokonanych przez podmiot przetwarzający koniecznych zmian może rozważyć zawarcie umowy powierzenia przetwarzania danych osobowych;**
3. **spełnienie przyjętych kryteriów na poziomie 49%** **i mniej** - podmiot przetwarzający nie daje wystarczającej gwarancji stosowania środków zapewniających spełnienie wymogów RODO i bezpieczeństwa praw osób, których dane dotyczą - **administrator nie powinien zawierać z takim podmiotem umowy powierzenia przetwarzania danych osobowych.**

*Wyżej przedstawione kryteria są instrumentem pomocniczym w procesie podejmowania decyzji dotyczącej powierzenia przetwarzania danych osobowych. Administrator dokonuje całościowej analizy uwzględniając wagę poszczególnych środków technicznych i organizacyjnych ujętych w liście kontrolnej jak i w całym procesie weryfikacyjnym podmiotu przetwarzającego.* ***Administrator powinien korzystać jedynie z takich podmiotów przetwarzających, które gwarantują wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających, że przetwarzanie spełnia wymogi RODO oraz chroni prawa osób, których dane są przetwarzane.***

Wypełniona lista kontrolna służy jako załącznik do umowy powierzenia przetwarzania danych, będąc jednocześnie dowodem stosowanych przez podmiot przetwarzający środków zapewniających zgodność przetwarzania z przepisami RODO oraz bezpieczeństwa przetwarzanych danych. Rozwiązanie takie jest właściwsze, w porównaniu do postanowień umownych, w ramach, których podmiot przetwarzający zobowiązuje się jedynie do stosowania odpowiednich środków.

1. **Niedopuszczalność powierzenia przetwarzania danych**

**W przypadku gdy podmiot, któremu administrator zamierza powierzyć przetwarzanie danych, nie jest w stanie spełnić wymogów dotyczących ochrony danych osobowych określonych w RODO, powierzenie przetwarzania danych takiemu podmiotowi jest niedopuszczalne.** Jeżeli pomimo to administrator dokona powierzenia przetwarzania danych takiemu podmiotowi, co stwierdzi organ nadzorczy, to administrator może ponieść odpowiedzialność za naruszenie przepisu art. 28 RODO w postaci administracyjnej kary pieniężnej w wysokości do 10 mln euro, a w przypadku przedsiębiorstwa - w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego rok obrotowego, przy czym zastosowanie ma kwota wyższa *(zgodnie z art. 83 ust. 4 RODO).*

1. **Zawarcie umowy powierzenia**

Zgodnie z art. 28 ust. 3 RODO przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy *(lub innego instrumentu prawnego)*, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora. Oznacza to, że **administrator - OKFiR Śmigiel oraz podmiot przetwarzający powinni zawrzeć umowę powierzenia przetwarzania** *(lub skorzystać z innego instrumentu prawnego).* **RODO wymaga, aby umowa powierzenia** *(lub inny instrument prawny)* **określały**:

1. **przedmiot przetwarzania** - będzie on powiązany z realizacją przedmiotu umowy głównej zawartej pomiędzy administratorem a podmiotem przetwarzającym*;*
2. **czas trwania przetwarzania** - co do zasady powiązany jest z realizacją przez podmiot zewnętrzny usługi na rzecz administratora w oparciu o umowę-zlecenie bądź świadczenia usług zawartą pomiędzy stronami;
3. **charakter przetwarzania** - rozumiany jako określenie następujących czynników przetwarzania danych osobowych: częstotliwości, powtarzalności, czasowości, długoterminowości, masowości z uwzględnieniem rodzajów zastosowanych technologii;
4. **cel przetwarzania** - określenie po co podmiot przetwarzający *(procesor)* ma przetwarzać dane osobowe w imieniu administratora;
5. **rodzaj danych osobowych** – należy wymienić jakie konkretnie dane osobowe będą podlegały powierzeniu przy uwzględnieniu podziału na dane zwykłe *(przykładowo wymienione w art. 4 pkt 1 RODO)* oraz dane szczególnych kategorii *(katalog zawarty w art. 9 ust. 1 RODO);*
6. **kategorię osób, których dane dotyczą** - sprecyzowanie grupy osób, których dane zostały powierzone do przetwarzania *np. pracowników, stażystów, dostawców;*
7. **obowiązki i prawa administratora** - w dużej części prawa administratora będą powiązane z realizacją obowiązków nałożonych na podmiot przetwarzający. Do obowiązków administratora określonych umownie można zaliczyć *np. sposób oraz termin przekazania do przetwarzania danych osobowych oraz udzielanie wszelkich informacji niezbędnych dla podmiotu przetwarzającego (procesora) do realizacji umowy powierzenia.*

**5.1** **Przepis art. 28 ust. 3 RODO wskazuje również bardziej szczegółowe wymogi dotyczące treści umowy** *(lub innego instrumentu prawnego)*, **stanowiące podstawę powierzenia. Powinny one w szczególności wskazywać, że podmiot przetwarzający:**

1. **przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora** – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej - chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
2. **zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy** lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3. **podejmuje środki techniczne i organizacyjne**, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku *(wymagane na mocy art. 32 RODO);*
4. **przestrzega warunków korzystania z usług innego podmiotu przetwarzającego** *(w przypadku tzw. podpowierzenia);*
5. biorąc pod uwagę charakter przetwarzania, w miarę możliwości **pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą**, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
6. uwzględniając charakter przetwarzania oraz dostępne mu informacje, **pomaga administratorowi wywiązać się z obowiązków związanych z: zabezpieczeniem danych, informowaniem o naruszeniach ochrony danych oraz dokonywaniem oceny skutków dla ochrony danych** *(określonych w art. 32–36 RODO);*
7. po zakończeniu świadczenia usług związanych z przetwarzaniem **zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie**, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
8. **udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków** oraz **umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów**, w tym inspekcji i przyczynia się do nich.

**Umowa** *(lub inny instrument prawny)* **powinny mieć - zgodnie z art. 28 ust. 9 RODO - formę pisemną, przy czym prawodawca unijny dopuścił formę elektroniczną.** Przepis art. 28 RODO przewiduje możliwość określenia standardowych klauzul umownych dotyczących powierzenia przetwarzania zarówno przez Komisję, jak i przez organ nadzorczy.

1. **Powierzenie a podpowierzenie danych**

Szczególnie istotnym zagadnieniem, koniecznym do uregulowania w ramach umowy powierzenia jest kwestia współpracy podmiotu przetwarzającego *(procesora)* z jego podwykonawcami odpowiedzialnymi za przetwarzanie powierzonych danych osobowych *(tzw. subprocesorami).* W pierwszej kolejności umowa powinna przesądzić o tym, czy podmiot przetwarzający ma w ogóle możliwość podpowierzenia danych administratora swoim podwykonawcom. W tym zakresie administrator może wyrazić ogólną zgodą na takie działania bądź uzależnić je od zgody szczególnej *(w zależności od konkretnego przypadku).* Umowa powierzenia powinna w szczególności precyzować: tryb wystąpienia o zgodą na podpowierzenie, w tym czas jej złożenia oraz termin jej wyrażenia *(należy bowiem pamiętać, że zgoda powinna mieć charakter uprzedni względem samej czynności podpowierzenia).* Zdaniem EROD **kluczową kwestia jest również, aby administrator posiadał wykaz wszystkich subprocesorów, z których usług korzysta podmiot przetwarzający.** **RODO przewiduje podpowierzanie wprost w art. 28 ust. 2 i 4, jednak pod warunkiem uzyskania szczególnej lub ogólnej pisemnej zgody administratora danych.** Przepisy RODO stanowią wprost, że odpowiedzialność za przetwarzanie danych przez subprocesora ponosi sam podmiot przetwarzający dane w imieniu administratora. Zgodnie bowiem z art. 28 ust. 4 RODO w sytuacji korzystania przez procesora z subprocesora, umowa pomiędzy tymi podmiotami winna nakładać na ten drugi te same obowiązki ochrony danych co w umowie zawartej pomiędzy administratorem a podmiotem przetwarzającym.

1. **Dopuszczalność przetwarzania danych przez podmiot przetwarzający**

Spełnienie wymogów określonych w art. 28 RODO sprawia, że przetwarzanie danych przez podmiot, któremu administrator zlecił przetwarzanie, jest dopuszczalne.

1. **Kiedy stosować umowę powierzenia?**

Powierzenie przetwarzania danych osobowych będzie miało miejsce w sytuacji, gdy podmiot zewnętrzny świadczy pewien rodzaj usług na rzecz administratora, z którymi związane jest przetwarzanie danych osobowych. Istota powierzenia przetwarzania danych osobowych jest ściśle powiązania z pojęciem outsourcingu, przez które należy rozumieć zlecenie podmiotowi zewnętrznemu *(wyspecjalizowanemu w określonej dziedzinie),* realizacji czynności związanych z funkcjonowaniem administratora. Można zatem wymienić następujące **przykłady sytuacji, w których co do zasady zobowiązani będziemy do zawarcia umowy powierzenia przetwarzania danych osobowych** *np.:*

1. *zewnętrzna obsługa księgowa;*
2. *zewnętrzna obsługa kadrowo - płacowa;*
3. *korzystanie z usług zewnętrznego archiwum;*
4. *zewnętrzne usługi niszczenia dokumentów;*
5. *świadczenie przez podmiot zewnętrznych usług IT (np. hosting, obsługa informatyczna …);*
6. *świadczenie usług ochrony obiektów w tym ich monitorowania przez podmiot zewnętrzny.*

**Zawarcie umowy powierzenia zależeć będzie także od tego, czy podmiot zewnętrzny - nasz usługodawca przetwarza dane osobowe jako podmiot przetwarzający czy jako odrębny administrator.**

Niniejsza Procedura obowiązuje od 22 października 2024 roku.

.

1. Rozporządzenie Parlamentu Europejskiego 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 *(ogólne rozporządzenie o ochronie danych -* ***RODO****).* [↑](#footnote-ref-1)