

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



123RF

[GIODO, o.s.](#)

Zgodnie z RODO, każdy podmiot musi samodzielnie oceniać ryzyko, jakie przetwarzanie danych osobowych może spowodować dla praw i wolności osób, których te dane dotyczą. To właśnie te wartości należy przede wszystkim brać pod uwagę - pisze GIODO.

Ogólne rozporządzenie o ochronie danych (RODO) nie odnosi się wprost do procesu zarządzania ryzykiem i nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie. Każdy podmiot musi dokonywać jej samodzielnie, uwzględniając wiele specyficznych dla niego czynników, takich jak: wielkość, struktura organizacyjna, możliwości techniczne czy zakres i rodzaj danych oraz cel ich przetwarzania. Jednym ze skutecznych systemowych sposobów dokonywania oceny ryzyka jest wdrożenie w danej jednostce procesu zarządzania ryzykiem.

Dla ułatwienia przyjęcia w tym zakresie właściwych rozwiązań, Generalny Inspektor Ochrony Danych Osobowych (GIODO), przygotował dwuczęściowy poradnik.

W pierwszej części, zatytułowanej Jak rozumieć podejście oparte na ryzyku według RODO?, eksperci GIODO wyjaśniają istotę zasady podejścia opartego na ryzyku oraz wskazują, do czego zasada ta zobowiązuje podmioty stosujące przepisy ogólnego rozporządzenia o ochronie danych. Tłumaczą też, czym jest ryzyko naruszenia praw i wolności osób, których dane dotyczą. Podkreślają przy tym, że szacowanie ryzyka to proces ciągły, który powinien być przeprowadzany przy użyciu konkretnej metody, zapewniającej jednocześnie stosowanie jednolitych definicji i pojęć.

W drugiej części, zatytułowanej Jak stosować podejście oparte na ryzyku?, przedstawione zostały kolejne możliwe etapy działań podejmowanych w celu przeprowadzania ogólnej oceny ryzyka oraz szczegółowej oceny ryzyka, czyli tzw. oceny skutków dla ochrony danych.