Czy jesteś gotowy na RODO?

GIODO
Generalny Inspektor Ochrony Danych Osobowych

2. Nowe podejście do ochrony danych osobowych

O ile podstawowe rozwiązania ogólnego rozporządzenia o ochronie danych osobowych trudno uznać za rewolucyjne, o tyle zaprezentowane w tym dokumencie podejście do ich praktycznego zastosowania jest już pewną rewolucją. Nie zmieniają się bowiem w sposób istotny podstawy prawne czy zasady przetwarzania danych osobowych. Jednak rewolucyjny charakter ma wprowadzenie nowych zasad, które zwiększają samodzielność, ale i odpowiedzialność administratorów danych.

W praktyce oznacza to np., że obecne przepisy przewidujące ogólny obowiązek zawiadamiania GIODO o przetwarzaniu danych osobowych (obowiązek zgłaszania zbiorów do rejestracji) przestają obowiązywać. W ich miejsce ogólne rozporządzenie wprowadza skuteczne procedury i mechanizmy koncentrujące się na tych operacjach przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Wyrażone w rozporządzeniu podejście oparte na ryzyku (ang. risk based approach) określa sposób, w jaki należy podchodzić do przetwarzania danych – w każdej sytuacji, kiedy zbieramy i korzystamy z danych osobowych, musimy przede wszystkim analizować ryzyko, jakie może to spowodować dla prywatności osób, których te dane dotyczą.

Zupełnie nową zasadą w systemie ochrony danych wprowadzoną przez rozporządzenie jest zasada rozliczalności (ang. accountability). Zgodnie z nią, na każdym administratorze danych spoczywa obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających zgodność w wymogami rozporządzenia (np. wprowadzenie rozwiązań umożliwiających realizację praw osób, których dane dotyczą). Rozporządzenie nie podaje jednak konkretnych przykładów najlepszych rozwiązań. Nie określa też minimalnych standardów technicznych mających na celu zabezpieczenie danych (zachęca jedynie do skorzystania z narzędzi pseudonimizacji czy też szyfrowania danych). Co istotne, przestanie też obowiązywać rozporządzenie MSWiA określające warunki techniczne i organizacyjne, jakie muszą spełniać urządzenia i systemy informatyczne wykorzystywane do przetwarzania danych osobowych. Od 25 maja 2018 r. każdy administrator - biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych - będzie musiał samodzielnie zdecydować, jakie zabezpieczenia, dokumentację i procedury przetwarzania danych wdrożyć.

Pomocne w podjęciu decyzji w tym zakresie mogą być wskazane w rozpo-rządzeniu instrumenty, takie jak zatwierdzane przez GIODO tzw. kodeksy postępowania, a także mechanizm certyfikacji, wytyczne Europejskiej Rady Ochrony Danych lub sugestie inspektora ochrony danych. Ponadto źródłem praktycznej i spraw-dzonej wiedzy w zakresie budowy i zarządzania środkami bezpieczeństwa mogą być również np. normy ISO.

Innym aspektem zasady rozliczalności jest wykazanie przez administratora przestrzegania prawa, np. poprzez udokumentowane wdrożenie instrumentów prawnych określonych w rozporządzeniu, takich jak przeprowadzona ocena skutków dla ochrony danych, wdrożenie zasady privacy by design i privacy by default lub też stosowanie przytoczonych wyżej zatwierdzonych kodeksów postępowania.