

## 1. Ustawa o cyberbezpieczeństwie

[Link](#)

28 sierpnia weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa, implementująca tzw. Dyrektywę NIS. Dyrektywa zobowiązuje państwa członkowskie do zapewnienia minimalnego poziomu cyberbezpieczeństwa poprzez m.in. nałożenie obowiązków na podmioty z sektora usług o krytycznym znaczeniu (infrastruktura cyfrowa, ochrona zdrowia, energetyka, bankowość, transport). Wystąpienie zdarzenia, które może mieć wpływ na cyberbezpieczeństwo, będzie wymagało wdrożenia odpowiednich działań dla zminimalizowania skutków incydentu i poinformowania o nim właściwego organu.

***Dostawcy usług krytycznych powinni śledzić prace nad rozporządzeniami wykonawczymi do ustawy, które określają w szczególności ich zadania.***

Cyberbezpieczeństwo | usługi cyfrowe

## 2. Transfer danych poza UE

[Link](#)

Rozporządzenie o Ochronie Danych Osobowych („RODO”) ogranicza możliwość transferu danych poza UE. Przekazywanie danych wymaga wdrożenia dodatkowych mechanizmów ochrony w ramach organizacji. Wyjątkiem są państwa, które Komisja Europejska uznała za zapewniające adekwatny poziom ochrony danych. Dotychczas, decyzje zostały wydane w stosunku do kilku państw (m.in. Kanada i Argentyna). Komisja ogłosiła we wrześniu projekt decyzji uznającej również Japonię za kraj odpowiednio chroniący dane osobowe. Znaczenie decyzji o adekwatności może znacząco wzrosnąć, jeżeli Trybunał Sprawiedliwości uzna inny mechanizm przekazywania danych (standardowe klauzule umowne) za nieadekwatne (jesienią ma zostać wydane orzeczenie w dotyczącej klauzul w sprawie C-311/18).

***Decyzje o adekwatności mają duże znaczenie, gdyż ułatwiają nawiązywanie stosunków gospodarczych z podmiotami w krajach trzecich.***

Transfer danych | RODO | TSUE

## 3. Komunikat Prezesa UODO w sprawie oceny skutków przetwarzania

[Link](#)

RODO zobowiązuje podmioty przetwarzające dane do przeprowadzenia oceny skutków dla ochrony danych. Ocena polega na dokładnym przeanalizowaniu planowanych operacji przetwarzania, dokonania oceny ryzyka takiego przetwarzania i zaplanowania środków, dla zminimalizowania potencjalnych niebezpieczeństw. Przeprowadzenie analizy jest niezbędne wtedy, gdy charakter przetwarzania szczególnie zagraża prywatności. Prezes UODO opublikował listę operacji, dla których przeprowadzenie oceny będzie obowiązkowe. Co ważne, w wykazie zostało wskazane, że operacji nie trzeba przeprowadzać dla monitoringu wizyjnego, jeżeli nagranie jest wykorzystywane wyłącznie dla analizy ewentualnych naruszeń prawa. Konieczność przeprowadzenia oceny co do monitoringu budziła wątpliwości z uwagi na brzmienie przepisu RODO, który mógł być interpretowany jako nakładający taki obowiązek.

***Przedsiębiorcy, planując operacje na danych, muszą sprawdzić, czy operacja nie została zamieszczona w wykazie.***

Orzecznictwo | RODO | TSUE

Na pytania odpowiadają:



**Agnieszka Wiercińska-Krużewska**  
senior partner  
[agnieszka.wiercinska@wkb.pl](mailto:agnieszka.wiercinska@wkb.pl)



**Karolina Miksa**  
senior associate  
[karolina.miksa@wkb.pl](mailto:karolina.miksa@wkb.pl)