

#6 Dekodując Akt w sprawie danych

Dziś pora na szósty wpis z cyklu #Dekodując Akt w sprawie danych. Zajmiemy się bardziej szczegółowo ochroną tajemnicy przedsiębiorstwa i wskażemy, jakie rozwiązania w tym zakresie może wdrażać posiadacz danych.

Czy posiadacz danych musi udostępniać Dane, które zawierają tajemnicę przedsiębiorstwa?

Posiadacz danych, co do zasady nie może odmówić udostępnienia Danych wyłącznie na tej podstawie, że niektóre z takich Danych stanowią jego tajemnicę przedsiębiorstwa (przypominamy, że: Dane stanowiące tajemnicę przedsiębiorstwa to dane, które nie są ujawnione do wiadomości publicznej, mają wartość gospodarczą a posiadacz podejmuje wobec nich działania, by zachować je w poufności).

Posiadacz ma prawo ochrony takich danych i w określonych sytuacjach odmowy lub wstrzymania udostępniania takich informacji.

Niniejszy materiał został przygotowany w celu poinformowania Klientów kancelarii o określonych istotnych zmianach w prawie polskim i nie stanowi on porady prawnej dotyczącej konkretnej sytuacji któregośkolwiek z Klientów i nie powinien być traktowany przez Klientów jako porada. W przypadku jakichkolwiek pytań związanych z przedstawionymi powyżej zagadnieniami prawnymi oraz ich możliwym wpływem na działalność gospodarczą danego Klienta w Polsce, prosimy o kontakt.

Jak posiadacz może chronić swoje tajemnice przedsiębiorstwa?

Posiadacz ma prawo wymagać od użytkownika i odbiorcy wdrożenia określonych zabezpieczeń organizacyjno-prawnych np.:

- umowy o zachowaniu w poufności (NDA),
- ścisłych protokołów dostępu,
- stosowania określonych standardów technicznych lub
- stosowania kodeksów postępowania.



Aby ochrona miała zastosowanie pamiętaj by wskazać w umowie udostępniania Danych, które konkretnie Dane będą zawierały tajemnicę przedsiębiorstwa. Dodatkowo, informacja czy mogą być generowane tajemnice przedsiębiorstwa musi być wskazana przed zawarciem umowy o świadczenie usług powiązanych.

Dla większej pewności, warto też rozważyć uwzględnienie w umowie z użytkownikiem prawa do audytu z udziałem niezależnych stron trzecich w celu weryfikacji, czy użytkownik wdrożył niezbędne środki w celu zapewnienia poufności Danych, które zawierają tajemnicę przedsiębiorstwa posiadacza danych.

Kiedy posiadacz danych może odmówić udostępnienia Danych, które zawierają tajemnicę przedsiębiorstwa?

Akt wprowadza dodatkową warstwę ochrony tzw. "hamulec ręczny tajemnicy przedsiębiorstwa", który określa warunki, na jakich posiadacz danych może wstrzymać lub zawiesić udostępnianie Danych (jeśli umowa już jest zawarta). Taka sytuacja jest dopuszczalna, gdy:

- nie osiągnięto porozumienia w sprawie niezbędnych środków technicznych,
- użytkownik nie wdrożył uzgodnionych zabezpieczeń lub
- udostępnianie grozi naruszeniem poufności tajemnic przedsiębiorstwa.

Jeśli wniosek o dostęp do danych zostanie przekazany do posiadacza, ale umowa nie zostanie jeszcze zawarta – posiadacz może odmówić udostępnienia danych w indywidualnych przypadkach - gdy pomimo środków technicznych i organizacyjnych podjętych przez użytkownika lub odbiorcę danych, ujawnienie tajemnic przedsiębiorstwa może spowodować poważne szkody gospodarcze.

W powyższych przypadkach posiadacz danych musi odpowiednio uzasadnić decyzję, przekazać ją w formie pisemnej oraz zawiadomić właściwy organ o jej podjęciu. Dane, które nie są chronione tajemnicą przedsiębiorstwa powinny zostać przekazane zgodnie z wnioskiem.



Jakie uprawnienia przysługują posiadaczowi w przypadku naruszenia tajemnicy przedsiębiorstwa?

Nie można też zapomnieć o treści art. 11 Aktu, z którego wynika, że posiadacz danych może stosować odpowiednie środki techniczne ochrony, takie jak inteligentne umowy i szyfrowanie, aby zapobiec nieuprawnionemu dostępowi do Danych (w tym metadanych) oraz zapewnić zgodność z przepisami Aktu i postanowieniami umownymi dotyczącymi udostępniania danych.

Środki te nie mogą jednak prowadzić do dyskryminacji odbiorców danych ani ograniczać praw użytkownika do uzyskania kopii, pobierania, wykorzystywania czy przekazywania danych osobom trzecim zgodnie z art. 5 Aktu. Użytkownicy, osoby trzecie i odbiorcy danych nie mogą zmieniać ani usuwać tych środków ochrony bez zgody posiadacza danych.

W przypadku naruszenia (np. uzyskania Danych podstępem, wykorzystania ich do nieuprawnionych celów, niezgodnego z prawem ujawnienia Danych, naruszenia uzgodnionych środków technicznych lub organizacyjnych), **posiadacz danych** (a w odpowiednich przypadkach także posiadacz tajemnicy przedsiębiorstwa lub użytkownik) **może żądać od osoby trzeciej lub odbiorcy danych:**

- usunięcia Danych i ich kopii,
- zaprzestania produkcji, oferowania lub wykorzystywania towarów, usług lub danych powstałych na podstawie nieuprawnionego wykorzystania,
- poinformowania użytkownika o naruszeniu oraz o podjętych środkach zaradczych,
- rekompensaty za poniesioną szkodę.

Powyższe konsekwencje a zwłaszcza usunięcie Danych i zaprzestanie produkcji mogą być szczególnie dotkliwe dla osoby trzeciej lub odbiorcy danych w związku z prowadzoną działalnością.



Jakie prawa przysługują użytkownikowi w przypadku bezzasadnej odmowy dostępu do Danych stanowiących tajemnice przedsiębiorstwa?

W przypadku odmowy, wstrzymania czy zawieszenia dzielenia się danymi w związku z ochroną tajemnic przedsiębiorstwa, użytkownik ma prawo wnieść skargę do właściwego organu wyznaczonego przez państwo członkowskie (koordynatora ds. danych), który podejmie decyzję, czy i na jakich warunkach dzielenie się danymi powinno się rozpocząć, zostać wznowione lub uzgodni z posiadaczem danych wniesienie sprawy do organu rozstrzygania sporów zgodnie z art. 10 ust. 1 Aktu (art. 4 ust. 9 Aktu). W takiej sytuacji, organ rozstrzygania sporów rozstrzygnie spór między posiadaczem danych a użytkownikiem. Takie same prawa przysługują osobom trzecim (art. 5 ust. 12 Aktu).

Naruszenie obowiązków określonych w Akcie podlega karom - państwa członkowskie są zobowiązane do ustanowienia skutecznych, proporcjonalnych i odstraszających sankcji, które mogą obejmować kary pieniężne, ostrzeżenia, nagany czy nakazy dostosowania praktyk biznesowych. Przy ustalaniu wysokości kary uwzględnia się m.in. charakter, wagę, czas trwania naruszenia, działania naprawcze oraz wcześniejsze naruszenia (art. 40 Aktu).

W kolejnym wpisie z cyklu [#Dekodując Akt w sprawie danych](#) zajmiemy się zagadnieniami związanymi z prawami i obowiązkami użytkownika danych. Stay tuned!

Zapraszamy do kontaktu!



Agata Szeliga

Partner, radca prawny

☎ +48 698 660 648

✉ agata.szeliga@skslegal.pl



Agnieszka Jurciewicz-Androsz

Prawnik, adwokat

☎ +48 600 782 823

✉ agnieszka.jurciewicz-androsz@skslegal.pl



Warszawa

Jasna 26, 00-054 Warszawa

T +48 22 608 70 00

F +48 22 608 70 70

E office@skslegal.pl

Katowice

Korfantego 138a, 40-156 Katowice

T +48 32 731 59 86

F +48 32 731 59 90

E office.katowice@skslegal.pl

Poznań

Mickiewicza 35, 60-837 Poznań

T +48 61 856 04 20

F +48 61 856 05 67

E office.poznan@skslegal.pl



SOŁTYSIŃSKI
KAWECKI
SZLĘZAK