

# Akt w sprawie danych (Data Act) - przewodnik

Warszawa, 26 września 2025 r.

Niniejsza publikacja służy wyłącznie celom informacyjnym i edukacyjnym i nie powinna być traktowana jako porada prawna.

W publikacji przedstawiono główne obowiązki nałożone na przedsiębiorców na mocy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych).

W tekście skupiono się na podkreśleniu potencjalnych nowych obowiązków dla przedsiębiorstw oraz nowych kompetencji organów rządowych. Nowe przepisy zostały przedstawione w formie skrótowej bez dodatkowej analizy.

© Copyright by Kobylańska Lewoszewski Mednis sp. j., 2025 r.

[www.klmlaw.pl](http://www.klmlaw.pl)

# Akt w sprawie danych – omówienie najważniejszych obowiązków

## 1. Wprowadzenie

Dane to złoto XXI w. a uwolnienie dostępu do nich stanowi jeden z kluczowych fundamentów rozwoju cyfrowej gospodarki Unii Europejskiej. W tym celu prawodawca unijny przyjął rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 zwane „aktem w sprawie danych” lub „**Data Act**”.

Jego celem jest „zapewnienie sprawiedliwego podziału wartości danych między podmiotami gospodarki opartej o dane oraz na ułatwienie dostępu do danych i ich wykorzystania”<sup>1</sup>. Jako że akt w sprawie danych został przyjęty w formie rozporządzenia, jest on bezpośrednio stosowany, bez wymogu uchwalenia ustawy implementującej i zaczął obowiązywać 12 września 2025 roku.

W opracowaniu przedstawiamy Państwu najważniejsze zagadnienia związane z wprowadzeniem Data Act. Przybliżamy w nim ogólne założenia, a także wymagania regulacyjne jakie nakłada ono na podmioty sektora prywatnego.

W razie jakichkolwiek pytań prosimy o kontakt.



**Marcin Lewoszewski**

Partner

Marcin.Lewoszewski@KLMLAW.PL

---

<sup>1</sup> Uzasadnienie do wniosku rozporządzenia w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystania, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022PC0068> (dostęp: 23.01.2025 r.).

## 2. Podstawowe pojęcia

Przed przystąpieniem do omówienia najważniejszych zagadnień Data Act, w kilku słowach należy przybliżyć pojęcia, którymi się on posługuje. Część pojęć pokrywa się już z dobrze znaną terminologią RODO. Dotyczy to m.in. definicji danych osobowych, przetwarzania danych, czy też osoby, której dane dotyczą. Jednakże akt w sprawie danych wprowadza też wiele nowych definicji.

W tej kwestii kluczowym wydaje się wyjaśnienie samego terminu **dane**. Na gruncie aktu oznaczają one wszelkie cyfrowe odwzorowania działań, faktów lub informacji oraz ich kompilacje wyrażone dźwiękowo, wizualnie lub audiowizualnie.

Inną definicją wymagającą przybliżenia jest **produkt skomunikowany** (ang. *connected product*). Są nimi wszystkie urządzenia zbierające lub generujące dane, których zadaniem jest ich przechowanie, przetwarzanie lub przesyłanie w imieniu użytkownika. Przykładami takich produktów są m.in. urządzenia *smart home* lub samochody podłączone do Internetu<sup>2</sup>. Wszystkie produkty tego typu będą podlegać regulacjom Data Act po ich wprowadzeniu na rynek UE.

Z omawianym terminem łączy się także pojęcie **usługi powiązanej** (ang. *related service*). Jest nią usługa cyfrowa, która jest połączona z działaniem produktu skomunikowanego<sup>3</sup> i wpływa na jego funkcjonalność, np. poprzez przesyłanie danych lub poleceń<sup>4</sup>. Musi zatem spełniać dwa wymogi – dwukierunkową wymianę danych (produkt skomunikowany ↔ dostawca usługi) oraz wpływać na działanie/funkcjonowanie/zachowanie się produktu skomunikowanego. Przykładem takiej usługi jest m.in. aplikacja z wbudowanymi odpowiednimi czujnikami, umożliwiającą kupującemu pralkę określanie, jaki wpływ na środowisko będą miały poszczególne cykle prania<sup>5</sup>.

Od usługi powiązanej należy odróżnić **usługę przetwarzania danych** (ang. *data processing service*). Obejmuje ona bowiem świadczenie usług w ramach tzw. chmury obliczeniowej, którą na gruncie Data Act zdefiniowano jako usługę cyfrową umożliwiającą swobodny dostęp

---

<sup>2</sup> Komisja Europejska, Akt w sprawie danych – wyjaśnienie, [https://digital-strategy.ec.europa.eu/pl/factpages/data-act-explained?utm\\_source=chatgpt.com](https://digital-strategy.ec.europa.eu/pl/factpages/data-act-explained?utm_source=chatgpt.com) (dostęp: 24.01.2025 r.).

<sup>3</sup> Produkt skomunikowany i usługa powiązana odnoszą się także do wirtualnych asystentów, którzy wchodzi w interakcję z tym produktem lub usługą. Wirtualnym asystentem jest z kolei oprogramowanie przetwarzające żądania, zadania lub pytania na podstawie dźwięku, pisma, gestu lub ruchu, na podstawie którego zapewnia dostęp do innych usług lub kontroluje funkcje produktu skomunikowanego.

<sup>4</sup> Komisja Europejska, Frequently Asked Questions. Data Act, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act> (dostęp: 10.02.2025 r.).

<sup>5</sup> <https://digital-strategy.ec.europa.eu/pl/factpages/data-act-explained> (dostęp 18.02.2025 r.)

do konfigurowalnych, skalowalnych i elastycznych zasobów obliczeniowych. Podmiotami świadczącymi tego typu usługi są **dostawcy usług przetwarzania**.

Zdefiniowano także podmioty objęte przepisami Data Act. Pierwszym z nich jest **użytkownik**, którym jest osoba fizyczna lub prawna znajdująca się na terytorium UE i będąca właścicielem produktu skomunikowanego lub usługi powiązanej. Użytkownikiem będzie też osoba, której na podstawie umowy, np. najmu lub leasingu, przysługuje prawo do korzystania z tego produktu lub usługi. Drugim ze zdefiniowanych podmiotów jest **posiadacz danych** (ang. *data holder*), którym jest osoba fizyczna lub prawna, która wykorzystuje lub udostępnia dane z produktu skomunikowanego lub usługi powiązanej podczas świadczenia usługi powiązanej. Wykorzystuje lub udostępnia on dane **odbiorcy danych** (ang. *data recipient*) – a więc osobie fizycznej lub prawnej prowadzącej działalność gospodarczą inną niż użytkownik.

### 3. Zakres stosowania Data Act

Jak wskazano w motywach aktu w sprawie danych, jego głównym założeniem jest rozwój europejskiego rynku danych oraz usunięcie barier w ich dostępie i wykorzystaniu. W związku z tym, Data Act reguluje udostępnianie danych w relacji:

- urządzenie ↔ osoba fizyczna/prawna (produkt/usługa powiązana ↔ użytkownik produktu skomunikowanego/usługi powiązanej),
- osoba fizyczna/prawna ↔ osoba fizyczna/prawna (posiadacz danych ↔ odbiorca danych),
- osoba fizyczna/prawna ↔ sektor publiczny (w tym organy UE), a także
- ułatwienie zmiany dostawcy usług przetwarzania danych.

W zakresie przedmiotowym Data Act obejmuje zarówno dane osobowe jak i nieosobowe<sup>6</sup>. Natomiast w kontekście podmiotowym do jego przestrzegania są zobowiązani:

- producenci produktów skomunikowanych i dostawcy usług powiązanych,
- użytkownicy produktów skomunikowanych i usług powiązanych,
- posiadacze i odbiorcy danych,
- dostawcy usług przetwarzania danych,
- uczestnicy przestrzeni danych oraz sprzedawcy aplikacji korzystających z inteligentnych umów, a także
- osoby, których działalność obejmuje wdrażanie inteligentnych umów.

Podkreślenia wymaga, że rozporządzenie nie będzie miało zastosowania do umów wzajemnych dotyczących dzielenia się lub wymiany danymi. Nie będzie miało także wpływu

---

<sup>6</sup> Danymi nieosobowymi są wszystkie dane inne niż dane osobowe.

na stosowanie przepisów RODO<sup>7</sup>. Niemniej jednak w niektórych przypadkach oba akty powinny być interpretowane łącznie. Dotyczy to m.in. przenoszenia danych z urządzeń Internatu Rzeczy (IoT). W przypadku kolizji przepisów zawsze jednak pierwszeństwo powinny znaleźć przepisy RODO.

#### **4. Dzielenie się danymi**

##### **4.1. Przepisy ogólne**

Kluczowym obszarem uregulowanym przez Data Act jest dzielenie się danymi, określane też jako ich udostępnianie. Wiąże się ono z wieloma obowiązkami nakładanymi na posiadaczy danych.

W tym kontekście, po pierwsze, wskazać należy, że produkty skomunikowane i usługi powiązane mają być projektowane i świadczone w taki sposób, aby dane (w tym metadane) z nich pochodzące były domyślnie łatwo, bezpiecznie, bezpłatnie i w całości dostępne dla użytkownika<sup>8</sup>. Wszystkie dane mają się nadawać do odczytu maszynowego. Dostęp ten jest prawem podmiotowym użytkownika. W przypadku bowiem, gdy nie uzyska on do nich bezpośredniego dostępu, może domagać się ich udostępnienia. Żądania dokonuje się w formie zwykłego wniosku elektronicznego<sup>9</sup>. Prawo to nie ma jednak charakteru absolutnego. Posiadacz danych wraz z użytkownikiem mogą je umownie ograniczyć lub zakazać dostępu/wykorzystania/dzielenia się danymi ze względu na:

- bezpieczeństwo produktu, a także
- negatywny wpływ na zdrowie, bezpieczeństwo lub ochronę osób fizycznych.

Na tak zastosowane ograniczenia umowne użytkownikowi będzie przysługiwać skarga do właściwego organu nadzoru.

##### **4.2. Tajemnica przedsiębiorstwa a udostępnianie danych<sup>10</sup>**

Udostępnianie danych nie może mieć negatywnego wpływu na poufność tajemnicy przedsiębiorstwa. Innymi słowy posiadacz danych może ograniczyć dostęp do niektórych danych, których udostępnienie naruszałoby tajemnicę przedsiębiorstwa. Musi on jednak

---

<sup>7</sup> Organy odpowiedzialne za przestrzeganie przepisów RODO będą także właściwe w zakresie przetwarzania danych osobowych na podstawie przepisów Data Act.

<sup>8</sup> Obowiązek ten nie dotyczy produktów skomunikowanych i usług powiązanych wytworzonych przez mikro i małych przedsiębiorstwa, pod warunkiem, że nie są one przedsiębiorstwami partnerskimi lub powiązanymi, a także nie są podwykonawcami danego produktu lub usługi. Preferencyjne uregulowania dotyczą również średnich przedsiębiorstw (prowadzących działalność przez okres krótszy niż rok), w pierwszym roku wprowadzenia przez nie do obrotu produktu skomunikowanego.

<sup>9</sup> Na wniosek użytkownika posiadacz danych udostępnia też dane osobie trzeciej.

<sup>10</sup> Zagadnienie to zostało omówione w pkt 23 dokumentu Komisji Europejskiej, Frequently Asked Questions. Data Act, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act> (dostęp.10.02.2025 r.).

dokonać wcześniejszej identyfikacji takich danych. Ponadto posiadacz danych ma obowiązek poinformować użytkownika, w formie pisemnej, o takim ograniczeniu udostępniania danych. W sytuacji, gdy nie wdrożył właściwych środków ochrony poufności tajemnicy przedsiębiorstwa, musi też poinformować o takim fakcie właściwy organ nadzoru. W tym kontekście skazać należy, że do takich środków należą: modelowe postanowienia umowne, umowy o poufność, protokoły ścisłego dostępu, normy techniczne oraz kodeksy postępowania.

#### **4.3. Obowiązki posiadaczy danych zobowiązanych do ich udostępniania**

W rozdziale II Data Act uregulowane zostały szczególne uprawnienia i obowiązki posiadaczy danych. Odnoszą się one w szczególności do udostępniania danych w relacji przedsiębiorca ↔ przedsiębiorca. W tym kontekście wskazać należy, że udostępnianie pomiędzy tymi podmiotami ma się odbywać na sprawiedliwych, rozsądnych i niedyskryminujących zasadach. Warunki takiego udostępniania wyznaczają stosowne umowy udostępniania danych. Przekazanie danych może wiązać się z określoną rekompensatą finansową, w tym również uwzględniać marżę.

W Data Act przewidziano także różnorodną ścieżkę rozwiązywania sporów pomiędzy posiadaczami i odbiorcami danych. Mogą być one bowiem rozstrzygane, nie tylko przez sądy powszechne, ale także odpowiednio certyfikowane organy (tzw. organ rozstrzygający spory). Jest to wprost wyrażona w rozporządzeniu możliwość dochodzenia swoich praw w formie pozasądowych metod rozwiązywania sporów.

Posiadacze danych mogą stosować także odpowiednie techniczne środki ochrony w celu ochrony przed nieuprawnionym dostępem do danych oraz uzgodnionymi postanowieniami umownymi w zakresie przekazywania danych. W tym kontekście mogą stosować m.in. inteligentne umowy czy też szyfrowanie.

#### **4.4. Udostępnianie danych podmiotom sektora publicznego**

W rozdziale V Data Act przewidziano szczególny rodzaj sytuacji, w których dane są udostępniane podmiotom sektora publicznego, w tym również Komisji Europejskiej, Europejskiego Banku Centralnego oraz innych instytucji UE. Jeśli instytucje te wykażą wyjątkową potrzebę wykorzystania określonych danych (w tym metadanych), w związku z realizacją swoich ustawowych obowiązków, podmioty posiadające te dane są zobowiązane do ich udostępnienia. Przez pojęcie wyjątkowej potrzeby należy rozumieć:

- niebezpieczeństwo publiczne<sup>11</sup>
- brak możliwości wykonania konkretnego zadania realizowanego w interesie publicznym (dotyczy tylko danych nieosobowych)<sup>12</sup>
- a także sytuację, gdy organ publiczny wyczerpał wszystkie inne dostępne sposoby pozyskiwania danych nieosobowych, w tym ich zakup poprzez zaoferowanie stawek rynkowych, a także powołania się na istniejące obowiązki udostępniania danych lub poprzez przejęcie nowych środków ustawodawczych, które mogłyby zagwarantować dostępność danych na czas.

Udostępnienia dokonuje się w oparciu o należycie uzasadniony wniosek. W jego ramach podmiot publiczny musi wyraźnie wskazać posiadaczowi danych m.in.:

- jakie dane (metadane) muszą zostać przekazane
- spełnienie warunków wyjątkowej potrzeby
- wyjaśnić cel wniosku oraz planowane wykorzystanie żądanych danych
- wskazać okres retencji danych
- uzasadnić wybór posiadacza danych
- wskazać podmioty sektora publicznego, z którymi pozyskane dane będą dzielone.

W oparciu o wniosek posiadacz danych ma obowiązek ich udostępnienia bez zbędnej zwłoki. W przypadku uznania przez posiadacza danych, że wniosek narusza jego prawa, przysługuje mu skarga do właściwego organu nadzoru. Ponadto może on odmówić uwzględnienia wniosku lub wystąpić o jego zmianę, gdy:

- nie ma kontroli nad żądanymi danymi
- podobny wniosek, w tym samym celu, złożył już inny podmiot publiczny
- wniosek nie spełnia wymogów określonych w stosownych przepisach Data Act.

Na złożenie sprzeciwu posiadacz danych ma 5 dni roboczych od dnia otrzymania wniosku dotyczącego udostępnienia danych ze względu na niebezpieczeństwo publiczne oraz 30 dni roboczych w pozostałych przypadkach.

Podkreślenia wymaga też, że udostępnianie danych osobowych podmiotom sektora publicznego wymaga ich wcześniejszego zanonimizowania przez posiadacza danych. Natomiast gdy żądanie dotyczy bezpośrednio danych osobowych, wtedy posiadacz danych

---

<sup>11</sup> Niebezpieczeństwo publiczne oznacza ograniczoną w czasie sytuację wyjątkową taką jak stan zagrożenia zdrowia publicznego, sytuację nadzwyczajną w wyniku klęski żywiołowej, poważną katastrofę spowodowaną przez człowieka, w tym poważny cyberincydent, która to sytuacja negatywnie wpływa na ludność UE i wiąże się z ryzykiem wystąpienia poważnych i trwałych następstw dla warunków życia lub stabilności gospodarczej, finansowej, i która zostaje oficjalnie ogłoszona zgodnie z prawem UE lub państwa członkowskiego.

<sup>12</sup> Obowiązek nie dotyczy mikro i małych przedsiębiorców.

musi dokonać ich pseudonimizacji. Ponadto za udostępnianie danych posiadacz danych może domagać się rekompensaty finansowej. Nie dotyczy to jednak sytuacji, gdy dane są przekazywane ze względu na niebezpieczeństwo publiczne<sup>13</sup>.

## 5. Dostawcy usług przetwarzania

### 5.1. Obowiązki dostawcy usług przetwarzania danych

W rozdziale VI Data Act zamieszczono uregulowania dotyczące zmiany dostawcy usług przetwarzania. W myśl przepisów aktu muszą oni ułatwiać klientom proces przeniesienia danych i zmianę dostawcy. Powinni usuwać także wszelkie przeszkody, takie jak ograniczenia przedkomercyjne, handlowe, techniczne, organizacyjne czy umowne, które utrudniają klientom:

- rozwiązanie umowy po okresie wypowiedzenia i pomyślne zakończenie zmiany dostawcy
- podpisanie nowej umowy z innym dostawcą
- przeniesienie danych i zasobów cyfrowych do innego dostawcy lub własnej infrastruktury ICT
- osiągnięcie porównywalnej funkcjonalności usług u nowego dostawcy
- oddzielenie różnych usług przetwarzania danych od innych usług przetwarzania danych świadczonych przez dostawcę, jeśli to technicznie możliwe.

Dostawcy usług przetwarzania danych muszą przestrzegać określonych zasad technicznych, w szczególności odnoszących się do przenoszenia danych oraz zapewnianie interoperacyjności między różnymi systemami. Obowiązki te dotyczą jedynie praktyk handlowych pierwotnego dostawcy usług.

Ponadto muszą zapewnić, aby umowy dotyczące świadczenia ich usług, w tym spoczywające na nich obowiązki oraz prawa klientów, były dostępne na piśmie i mogły być przechowywane przez użytkowników. Powinni oni także mieć możliwość zapoznania się z nimi jeszcze przed podpisaniem umowy.

Umowa powinna jasno określać:

- **czas na przeniesienie danych** - użytkownik ma prawo przenieść dane do innego dostawcy lub lokalnej infrastruktury ICT w ciągu określonego czasu, nie później niż po upływie obowiązkowego maksymalnego okresu przejściowego wynoszącego 30 dni kalendarzowych i rozpoczynającego się po maksymalnym okresie wypowiedzenia nieprzekraczającym dwóch miesięcy

---

<sup>13</sup> Wyjątkiem jest sytuacja, gdy wniosek kierowany jest do mikro lub małego przedsiębiorcy.

- **wsparcie techniczne** - dostawca ma obowiązek pomóc użytkownikowi w przenoszeniu danych, np. poprzez udostępnienie odpowiednich narzędzi lub instrukcji.
- **potencjalne ryzyko** - dostawca powinien poinformować użytkownika o możliwych zagrożeniach czy ograniczeniach związanych z procesem przenoszenia danych, takich jak potencjalna utrata lub czasowa niedostępność usług
- **kategorie danych** – dostawca powinien określić szczegółową specyfikację wszystkich kategorii danych i aktywów cyfrowych<sup>14</sup>, które klient może przenieść.
- **działania klienta po zakończeniu umowy** - zmiana dostawcy, przejście na lokalną infrastrukturę ICT lub usunięcie danych
- **postępowanie w przypadku technicznej niemożliwości zachowania okresu przejściowego** – w przypadku problemów technicznych dostawca musi uzasadnić sytuację i zaproponować alternatywny okres (maks. 7 miesięcy), zapewniając ciągłość usług.

Dostawcy usług przetwarzania danych muszą informować klientów o procedurach zmiany dostawcy, metodach i formatach przenoszenia danych oraz technicznych ograniczeniach, jakie mogą wystąpić. W szczególności muszą informować o strukturach danych, formatach oraz otwartych standardach umożliwiających interoperacyjność. Ponadto wszystkie strony zaangażowane w proces zmiany dostawcy, w tym nowy dostawca usług, mają obowiązek współpracować w dobrej wierze. Ich celem jest zapewnienie płynnego i terminowego przenoszenia danych oraz utrzymanie ciągłości usług przetwarzania danych podczas zmiany dostawcy.

Dostawcy muszą także zachować przejrzystość dotyczącą dostępu międzynarodowego. Oznacza to, że są obowiązani regularnie publikować na swoich stronach internetowych informacje o:

- jurysdykcji, której podlega infrastruktura przetwarzania danych oraz
- zastosowanych środkach technicznych i organizacyjnych, które chronią dane przed nieuprawnionym dostępem z zagranicy lub przekazaniem ich administracji rządowej.

---

<sup>14</sup> Aktywami cyfrowymi na gruncie Data Act są elementy w formacie cyfrowym, w tym aplikacje, z których klient ma prawo korzystać niezależnie od stosunku umownego obejmującego usługę przetwarzania danych, której dostawcę zamierza zmienić.

## 5.2. Opłaty z tytułu zmiany dostawcy



W okresie od **11 stycznia 2024 roku do 12 stycznia 2027** roku opłaty mogą być nakładane, ale muszą być obniżone i ograniczone wyłącznie do rzeczywistych kosztów poniesionych w związku z przenoszeniem danych.

Od **12 stycznia 2027** roku dostawcy nie mogą nakładać żadnych opłat za zmianę dostawcy usług.

## 5.3. Techniczne aspekty zmiany dostawcy usług przetwarzania danych

Dostawcy usług przetwarzania danych, zajmujący się obsługą infrastruktury, z wyłączeniem usług operacyjnych, oprogramowania i aplikacji, powinni zapewnić, aby klienci, zmieniając dostawcę, zachował funkcjonalność swoich danych i usług u nowego dostawcy, oferując zasoby, dokumentację, wsparcie techniczne i niezbędne narzędzia.

Pozostali dostawcy usług przetwarzania danych są zobowiązani **nieodpłatnie** udostępnić klientom i docelowym dostawcom otwarte interfejsy, umożliwiające przenoszenie i interoperacyjność danych. Ponadto dostawcy będą zobligowani do zapewnienia zgodności ze wspólnymi specyfikacjami opartymi na otwartych standardach interoperacyjności lub zharmonizowanych normach interoperacyjności. Dostawcy usług przetwarzania danych nie są zobowiązani do tworzenia nowych technologii, udostępniania chronionych zasobów cyfrowych objętych prawami własności intelektualnej lub tajemnicą przedsiębiorstwa. Nie mogą także podejmować działań, które mogłyby narazić bezpieczeństwo i integralność usług klienta lub innego dostawcy.

Powyższe obowiązki nie mają jednak zastosowania, jeśli:

- usługi są dostosowywane na zamówienie do specyficznych potrzeb konkretnego klienta
- wszystkie komponenty usług zostały opracowane wyłącznie na potrzeby danego klienta i nie są oferowane komercyjnie na szeroką skalę, a także gdy
- dana usługa stanowi wersję testową, która jest dostępna tylko przez ograniczony czas.

Dostawcy muszą poinformować klientów o wszelkich wyłączeniach z obowiązków przed podpisaniem umowy.

#### **5.4. Międzynarodowy dostęp administracji rządowej i przekazywanie danych**

Dostawcy usług przetwarzania danych muszą stosować odpowiednie środki techniczne, organizacyjne i prawne, aby chronić dane przed:

- nieuprawnionym dostępem administracji rządowej spoza UE
- nielegalnym przekazywaniem danych poza UE

Dostęp do danych na podstawie nakazów z państw spoza UE może być uznany za zgodny z prawem tylko wtedy, gdy:

- istnieje odpowiednia umowa międzynarodowa między UE a danym państwem trzecim
- w przypadku otrzymania wniosku o dostęp do danych, dostawca musi poinformować klienta, chyba że wniosek dotyczy ścigania przestępstw i wymaga poufności.

W przypadku koniecznego przekazania dostawca musi ograniczyć ilość przekazywanych danych do niezbędnego minimum. Dodatkowo zanim je przekaże, powinien poinformować klienta o wniosku, chyba że wniosek dotyczy ścigania przestępstw i wymaga zachowania poufności.

Adresat decyzji lub orzeczenia może poprosić odpowiedni organ krajowy o opinię, aby sprawdzić czy spełniono warunki dotyczące przekazania danych, szczególnie jeśli uważa, że sprawa dotyczy tajemnic przedsiębiorstwa, danych handlowych, własności intelektualnej lub ryzyka deanonimizacji. Jeśli adresat uzna, że decyzja może zagrozić bezpieczeństwu narodowemu lub interesom obronnym UE lub jej państw członkowskich, powinien wówczas zwrócić się o opinię do właściwych organów krajowych. Jeśli nie otrzyma odpowiedzi w ciągu miesiąca lub opinia potwierdzi, że warunki nie zostały spełnione, może odmówić przekazania danych.

#### **6. Wymagania w zakresie interoperacyjności danych**

Uczestnicy przestrzeni danych oferują dane lub usługi oparte na danych (w tym również usługi przetwarzania danych) spełniające wymogi interoperacyjności wskazane w Data Act. Obejmują one m.in. właściwy opis zestawu danych w zakresie ich zawartości, ograniczeń wykorzystania, licencji, metod zbierania danych i ich jakości, struktury danych, technicznych środków dostępu.

Interoperacyjność ma ułatwić opracowywanie nowych produktów i usług, prowadzenie badań naukowych

i poprawę inicjatyw społeczeństwa obywatelskiego. W tym celu dostarczane dane muszą być dostatecznie opisane m.in. w zakresie zawartości zestawu danych, ograniczenia ich wykorzystania, czy też metody ich zbierania.

## 7. Wymagania dotyczące inteligentnych umów

Dostawcy aplikacji lub osoby wdrażające inteligentne umowy muszą zapewnić:

- **odporność i kontrolę dostępu** – ochrona przed błędami i manipulacją osób trzecich
- **bezpieczne zakończenie** – możliwość przerwania działania w razie potrzeby
- **archiwizację i ciągłość danych** – zachowanie zapisów transakcji i kodu
- **spójność** – zgodność z umowami o dzieleniu się danymi

## 8. Właściwe organy i koordynatorzy danych

Państwa członkowskie są zobowiązane do wyznaczenia właściwych organów odpowiedzialnych za egzekwowanie przepisów Data Act. W przypadku wyznaczenia kilku organów należy wskazać koordynatora danych, który będzie pełnił rolę centralnego punktu kontaktowego, ułatwiając współpracę między organami i wspieranie podmiotów objętych zakresem rozporządzenia.

Właściwe organy są odpowiedzialne za monitorowanie przestrzegania przepisów, rozpatrywanie skarg, prowadzenie postępowań oraz nakładanie skutecznych i proporcjonalnych kar pieniężnych. Mają również obowiązek propagowania wiedzy na temat praw i obowiązków wynikających z Data Act, a także monitorowania postępu technologicznego i sytuacji gospodarczej istotnych dla udostępniania i wykorzystania danych.

Koordynator danych działa jako centralny punkt kontaktowy, udostępniający w formie elektronicznej wnioski organów publicznych o dostęp do danych. Będzie również promował dobrowolne umowy o udostępnianiu danych między organami publicznymi a posiadaczami danych. Ponadto koordynator, co roku, będzie informował Komisję o odmowach udzielenia dostępu do danych.

Dodatkowo, właściwe organy mają prawo żądać od podmiotów wszelkich informacji niezbędnych informacji do weryfikacji przestrzegania rozporządzenia, przy czym takie wnioski muszą być proporcjonalne i odpowiednio uzasadnione. W sytuacji, gdy organ jednego państwa członkowskiego zwraca się o pomoc do organu w innym państwie, wniosek musi być uzasadniony, a odpowiedź powinna być udzielona bez zbędnej zwłoki.

## 9. Prawo do wniesienia skargi

Każda osoba fizyczna i prawna będzie mogła złożyć skargę do odpowiednich organów, jeśli jej prawa wynikające z Data Act zostaną naruszone. Organy nadzoru będą musiały informować składających skargi o przebiegu postępowania i podjętych decyzjach, a w przeciwnym razie osoba składająca skargę będzie mogła skorzystać z sądowego środka ochrony prawnej lub kontroli. Skarżącym będzie też przysługiwać prawo odwołania się od decyzji organów do sądu.

## 10. Kary

Obowiązek ustanawiania przepisów dotyczących kar przyznano kompetencji państw członkowskich. Do dnia 12 września 2025 r. państwa muszą poinformować Komisję Europejską o swoich przepisach dotyczących kar oraz na bieżąco aktualizować te informacje.

Kryteria, które będą uwzględniane przy nakładaniu kar:

- skala i powaga naruszenia
- działania naprawcze podjęte przez naruszającego
- powtarzalność naruszeń
- uzyskane korzyści finansowe lub uniknięte straty
- roczny obrót naruszającego w poprzednim roku budżetowym

Kary będą nakładane za naruszenia obowiązków dotyczących:

- dzielenia się danymi przez przedsiębiorców z konsumentami i z innymi przedsiębiorcami
- obowiązków posiadaczy danych zobowiązanych do udostępnienia danych zgodnie z prawem Unii
- udostępniania danych organom sektora publicznego, w tym Komisji Europejskiej, Europejskiemu Bankowi Centralnemu i organom Unii.

Organy nadzorcze odpowiedzialne za monitorowanie stosowania RODO będą mogły nałożyć administracyjną karę pieniężną zgodnie z art. 83 RODO do wysokości 20 mln euro lub w przypadku przedsiębiorstw 4% całkowitego światowego rocznego obrotu.

W razie jakichkolwiek pytań, prosimy o kontakt.



**Marcin Lewoszewski**

Partner

[Marcin.Lewoszewski@KLMLAW.PL](mailto:Marcin.Lewoszewski@KLMLAW.PL)

## O nas

Stworzyliśmy wyspecjalizowaną kancelarię prawną, aby pomóc naszym klientom w ochronie ich wartości niematerialnych i prawnych oraz w rozwijaniu nowego biznesu w oparciu o nowe technologie i dane. Naszym celem jest kompleksowe, specjalistyczne wsparcie w kluczowych kwestiach naszych Klientów – jesteśmy stale blisko nich, udzielając najbardziej precyzyjnych, przejrzystych i zorientowanych na biznes porad prawnych – zawsze dostosowanych do ich potrzeb biznesowych.

Bazujemy na naszym wieloletnim doświadczeniu, zdobytym w uznanych międzynarodowych kancelariach prawnych działających w Polsce.

Oferujemy wsparcie prawne w zakresie dostosowania praktyk biznesowych do wymogów bezpieczeństwa danych, przepisów o ochronie danych osobowych, w szczególności w kontekście RODO, Data Act, NIS2, Digital Services Act, CER i innych przepisów.

