WZORZEC DOKUMENTU · UMOWY.AI

Umowa o zachowaniu poufności

Mutual NDA · współpraca B2B · branża IT

Pełna dwustronna umowa NDA wygenerowana z odniesieniem do polskiego Kodeksu cywilnego, ustawy o zwalczaniu nieuczciwej konkurencji oraz RODO. Treść tworzona od zera w trybie Behemoth — z badaniem przepisów, orzecznictwa SAOS i bieżącej praktyki kontraktowej.

TYP DOKUMENTU	Mutual NDA · B2B · IT
TRYB GENERACJI	Behemoth
REVIEWER JAKOŚCI	Claude Opus 4.8 (Anthropic)
ŹRÓDŁA WYKORZYSTANE	12 cytowanych pozycji · 5 przepisów · 1 orzeczenie · 6 badań praktyki
WYWOŁANIA API	130 · 1,6 mln tokenów
CONFIDENCE SCORE	0,85 / 1,00
DATA WYGENEROWANIA	15 czerwca 2026
CZAS PRACY SYSTEMU	~56 minut

Dokument zachowuje wszystkie cytowania [1] [10] [33] w formie kolorowych pigułek odpowiadających typowi źródła. Pełna bibliografia dostępna na końcu wzorca.

Spis treści

Siedem paragrafów uregulowanych w oparciu o art. 11 UZNK, art. 353[1], art. 72[1], art. 483 § 1 KC oraz aktualną praktykę kontraktową NDA w IT.

§ 1

Strony umowy i charakter relacji

1. Niniejsza umowa zostaje zawarta pomiędzy: 1) [pełna firma/nazwa Strony A], [forma prawna], z siedzibą / adresem głównego miejsca wykonywania działalności w [adres], wpisaną do [KRS / CEIDG] pod numerem [numer], NIP: [numer], REGON: [numer, opcjonalnie], reprezentowaną przez [imię i nazwisko, funkcja] działającego/działającą na podstawie [zasad reprezentacji ujawnionych we właściwym rejestrze / pełnomocnictwa], zwaną dalej „Stroną A", 2) [pełna firma/nazwa Strony B], [forma prawna], z siedzibą / adresem głównego miejsca wykonywania działalności w [adres], wpisaną do [KRS / CEIDG] pod numerem [numer], NIP: [numer], REGON: [numer, opcjonalnie], reprezentowaną przez [imię i nazwisko, funkcja] działającego/działającą na podstawie [zasad reprezentacji ujawnionych we właściwym rejestrze / pełnomocnictwa], zwaną dalej „Stroną B" [3] [4].

2. Strona A i Strona B łącznie zwane są dalej „Stronami", a każda z osobna „Stroną". Strony oświadczają, że zawierają niniejszą umowę jako przedsiębiorcy w relacji B2B oraz że osoby podpisujące umowę są należycie umocowane do jej zawarcia [3] [4].

3. Umowa ma charakter dwustronny i wzajemny (mutual NDA), co oznacza, że każda ze Stron może, zależnie od okoliczności danego przypadku, występować zarówno jako strona ujawniająca informacje poufne, jak i jako strona otrzymująca informacje poufne, a obowiązki poufności mają wobec obu Stron charakter równorzędny [1].

4. Na potrzeby niniejszej umowy „Strona Ujawniająca" oznacza Stronę, która w danym przypadku ujawnia drugiej Stronie informacje poufne, natomiast „Strona Otrzymująca" oznacza Stronę, która takie informacje otrzymuje. Określenia te mają charakter funkcjonalny i odnoszą się do konkretnego przepływu informacji, a nie do stałego przypisania roli do jednej ze Stron [1].

5. Strony zgodnie potwierdzają, że ujawnianie informacji poufnych następuje lub może następować w związku z prowadzonymi negocjacjami, analizą przedwdrożeniową, testami, proof of concept (PoC), planowaną współpracą, wdrożeniem, utrzymaniem albo realizacją projektu IT, wyłącznie w zakresie niezbędnym do oceny, przygotowania, zawarcia lub wykonywania tej współpracy [1] [2].

6. W przypadku gdy którakolwiek ze Stron działa przez pełnomocnika, do umowy należy dołączyć pełnomocnictwo albo wyraźnie wskazać dane pełnomocnika oraz zakres jego umocowania. W razie rozbieżności pomiędzy treścią umowy a danymi ujawnionymi we właściwym rejestrze pierwszeństwo mają dane identyfikacyjne i zasady reprezentacji wynikające z tego rejestru lub z ważnego dokumentu pełnomocnictwa [4].

PODSTAWA PRAWNA
Kodeks cywilny (k.c.)

§ 2

Definicje informacji poufnych i wyłączenia

1. Na potrzeby Umowy „Informacje Poufne” oznaczają wszelkie informacje, dane i materiały ujawnione, przekazane lub udostępnione przez jedną Stronę drugiej Stronie w związku z negocjacjami, analizą przedwdrożeniową, testami, wdrożeniem lub realizacją współpracy, niezależnie od ich formy, sposobu utrwalenia lub sposobu udostępnienia, w szczególności w formie ustnej, pisemnej, elektronicznej, wizualnej, na nośnikach danych, w korespondencji, podczas spotkań, prezentacji, demo, warsztatów, w systemach informatycznych, środowiskach, repozytoriach, narzędziach projektowych lub poprzez umożliwienie dostępu do nich [1] [8] [9].

2. Informacje Poufne obejmują w szczególności: 1) kod źródłowy, kod wynikowy, skrypty, biblioteki, moduły, konfiguracje, klucze techniczne, dane dostępowe i pliki elektroniczne; 2) repozytoria kodu, branch’e, commit’y, backlogi, roadmapy, tickety, harmonogramy, wyniki testów, logi, raporty oraz modele danych; 3) dokumentację techniczną, projektową, bezpieczeństwa i utrzymaniową, w tym specyfikacje, architekturę systemów, integracje, API, interfejsy, schematy, diagramy i procedury; 4) dokumentację biznesową i handlową, w tym oferty, cenniki, kalkulacje, warunki współpracy, marże, założenia projektowe i informacje o klientach lub kontrahentach; 5) know-how, informacje organizacyjne, technologiczne i inne informacje posiadające wartość gospodarczą, w tym informacje mogące stanowić tajemnicę przedsiębiorstwa [8] [9].

3. Oznaczenie informacji jako poufnych jest zalecane dla celów dowodowych, jednak brak takiego oznaczenia nie wyłącza ochrony, jeżeli z charakteru informacji, celu ich ujawnienia, sposobu ich przekazania albo okoliczności współpracy rozsądnie wynika, że powinny być traktowane jako poufne [8] [9]. Dotyczy to także informacji ujawnionych ustnie, podczas spotkań roboczych, prezentacji, rozmów handlowych, sesji discovery, przeglądów kodu, demo lub w toku dostępu do systemów i środowisk Strony ujawniającej [9].

4. Nie stanowią Informacji Poufnych wyłącznie te informacje, co do których Strona otrzymująca wykaże, że: 1) były publicznie znane lub stały się publicznie dostępne bez naruszenia Umowy lub bezprawnego działania Strony otrzymującej albo osób, za które ponosi ona odpowiedzialność; 2) były legalnie posiadane przez Stronę otrzymującą przed ich ujawnieniem przez drugą Stronę; 3) zostały opracowane niezależnie, bez wykorzystania Informacji Poufnych drugiej Strony; 4) zostały legalnie uzyskane od osoby trzeciej uprawnionej do ich ujawnienia i nieobjętej wobec nich obowiązkiem poufności; albo 5) ich ujawnienie jest wymagane przez bezwzględnie obowiązujące przepisy prawa, prawomocne orzeczenie sądu lub decyzję innego uprawnionego organu [1] [8] [9].

5. Strona powołująca się na którekolwiek z wyłączeń, o których mowa powyżej, jest zobowiązana wykazać jego zaistnienie wiarygodnymi dowodami, w szczególności dokumentacją, korespondencją, logami systemowymi, historią repozytorium, zapisami projektowymi, ofertami lub innymi danymi utrwalonymi przed datą otrzymania danej informacji [1] [9].

6. W przypadku ujawnienia Informacji Poufnych wymaganego prawem lub aktem uprawnionego organu Strona otrzymująca: 1) ujawni informacje wyłącznie w minimalnym zakresie prawnie wymaganym; 2) o ile jest to prawnie dopuszczalne, niezwłocznie poinformuje drugą Stronę o

żądaniu ujawnienia, jego podstawie i przewidywanym zakresie; oraz 3) podejmie uzasadnione działania w celu zapewnienia dalszej ochrony poufności ujawnianych informacji [1] [8] [9].

PODSTAWA PRAWNA
Kodeks cywilny (k.c.) · Ustawa o zwalczaniu nieuczciwej konkurencji (UZNK) · Badanie praktyki kontraktowej

§ 3
Cel ujawniania i dozwolony zakres wykorzystania

1. Strony zgodnie postanawiają, że wszelkie Informacje Poufne mogą być ujawniane i wykorzystywane wyłącznie w celu oceny, przygotowania, negocjowania, zawarcia, wdrożenia, wykonywania lub utrzymania planowanej albo realizowanej współpracy gospodarczej lub projektu między Stronami, w tym w szczególności projektu z obszaru IT (dalej: „Cel") [1] [12].

2. Odbiorca może korzystać z Informacji Poufnych wyłącznie w zakresie niezbędnym do realizacji Celu. Jakiekolwiek użycie Informacji Poufnych do innego celu, choćby pośrednio, wymaga uprzedniej zgody drugiej Strony wyrażonej co najmniej w formie dokumentowej [1] [8].

3. Bez uprzedniej zgody drugiej Strony zabronione jest w szczególności wykorzystywanie Informacji Poufnych: 1) w działalności konkurencyjnej wobec drugiej Strony; 2) do tworzenia, rozwijania, testowania, trenowania, oferowania lub komercjalizacji rozwiązań, produktów albo usług konkurencyjnych wobec rozwiązań, produktów albo usług drugiej Strony; 3) na potrzeby innych projektów, klientów lub postępowań zakupowych niezwiązanych z Celem [1] [8] [10].

4. Kopiowanie, powielanie, utrwalanie, pobieranie, drukowanie, eksportowanie, rozpowszechnianie lub inne zwielokrotnianie Informacji Poufnych jest dopuszczalne wyłącznie w zakresie niezbędnym do realizacji Celu oraz wyłącznie dla osób, które muszą mieć do nich dostęp w związku z realizacją Celu. Niedopuszczalne jest tworzenie kopii zapasowych, zestawień, ekstraktów, zrzutów, eksportów danych lub innych utrwaleń ponad zakres obiektywnie niezbędny do realizacji Celu [1] [8] [12].

5. Ujawnienie Informacji Poufnych nie stanowi przeniesienia na Odbiorcę jakichkolwiek praw własności intelektualnej, praw do wyników prac, know-how, autorskich praw majątkowych ani udzielenia licencji, sublicencji lub innego uprawnienia do korzystania z Informacji Poufnych, dokumentacji, kodu źródłowego, kodu wynikowego, architektury systemu, interfejsów API, modeli, makiet, repozytoriów, danych testowych lub innych materiałów, chyba że Strony wyraźnie postanowią inaczej w odrębnej umowie [1] [12].

6. Dla uniknięcia wątpliwości Strony potwierdzają, że użycie Informacji Poufnych poza Celem, w szczególności w sposób wskazany w ust. 3 lub 4, stanowi naruszenie niniejszej Umowy i może równocześnie naruszać tajemnicę przedsiębiorstwa drugiej Strony [8] [10].

PODSTAWA PRAWNA
Kodeks cywilny (k.c.) · Ustawa o zwalczaniu nieuczciwej konkurencji (UZNK) · orz. I AGa 336/22 (Sąd Apelacyjny) · Praktyka kontraktowa NDA B2B (PL)

§ 4
Dostęp do informacji i środki bezpieczeństwa

1. Każda ze Stron może udostępniać Informacje Poufne wyłącznie swoim pracownikom, współpracownikom, podwykonawcom oraz doradcom, i tylko w zakresie, w jakim osoby te muszą znać takie informacje dla potrzeb negocjowania, przygotowania, wdrożenia, wykonania lub utrzymania współpracy objętej Umową. Dostęp do Informacji Poufnych powinien być nadawany imiennie, zgodnie z zakresem obowiązków, oraz niezwłocznie odbierany po ustaniu potrzeby biznesowej uzasadniającej dostęp. 1 8 16

2. Przed uzyskaniem dostępu do Informacji Poufnych każda osoba, o której mowa w ust. 1, musi być związana obowiązkiem zachowania poufności oraz obowiązkiem stosowania środków bezpieczeństwa co najmniej równoważnych wynikającym z niniejszej Umowy, na podstawie umowy, obowiązujących regulacji wewnętrznych albo innego wiążącego zobowiązania. Każda ze Stron ponosi odpowiedzialność za działania i zaniechania tych osób jak za działania i zaniechania własne. 1 10

3. Każda ze Stron zobowiązuje się stosować przy przetwarzaniu, przechowywaniu i przekazywaniu Informacji Poufnych co najmniej następujące środki bezpieczeństwa: 1) kontrolę dostępu opartą na rolach i zasadzie need-to-know; 2) indywidualne konta użytkowników oraz uwierzytelnianie wieloskładnikowe (MFA) dla systemów zawierających Informacje Poufne oraz dla dostępu zdalnego; 3) szyfrowanie Informacji Poufnych w transmisji oraz, jeżeli jest to uzasadnione charakterem nośnika lub środowiska, także w przechowywaniu; 4) korzystanie wyłącznie z autoryzowanych i odpowiednio zabezpieczonych kanałów komunikacji oraz narzędzi; 5) ograniczenia pobierania, kopiowania, drukowania, eksportu i dalszego rozpowszechniania do minimum niezbędnego dla celu Umowy; 6) rejestrowanie dostępu i istotnych operacji na Informacjach Poufnych; 7) bezpieczne przechowywanie nośników i urządzeń zawierających Informacje Poufne oraz ochronę przed dostępem osób nieuprawnionych. 8 16

4. Zabronione jest w szczególności: 1) ujawnianie, współdzielenie albo przekazywanie danych logowania lub korzystanie ze wspólnych kont użytkowników; 2) używanie nieautoryzowanych aplikacji, komunikatorów, prywatnych skrzynek pocztowych, prywatnych repozytoriów, prywatnych kont chmurowych lub innych niezatwierdzonych narzędzi do przechowywania albo przekazywania Informacji Poufnych; 3) przenoszenie Informacji Poufnych do środowisk niezabezpieczonych, testowych lub prywatnych bez uprzedniego zapewnienia środków ochrony nie niższych niż wymagane na podstawie niniejszej Umowy; 4) obchodzenie lub wyłączanie uzgodnionych zabezpieczeń technicznych i organizacyjnych. 8 16

5. Każda ze Stron zobowiązuje się niezwłocznie, nie później niż w terminie 24 godzin od stwierdzenia zdarzenia, poinformować drugą Stronę o każdym incydencie bezpieczeństwa, utracie danych, utracie nośnika, naruszeniu poufności albo podejrzeniu nieuprawnionego dostępu do Informacji Poufnych. Zawiadomienie powinno obejmować co najmniej opis zdarzenia, wstępnie ustalony zakres i możliwe skutki naruszenia, podjęte działania zabezpieczające oraz plan dalszych czynności. Strona, u której wystąpiło zdarzenie, zobowiązana jest ponadto niezwłocznie ograniczyć jego skutki, zabezpieczyć dowody oraz współpracować z drugą Stroną przy wyjaśnieniu okoliczności zdarzenia. [16]

6. Jeżeli Informacje Poufne obejmują dane osobowe, każda ze Stron zobowiązuje się stosować środki bezpieczeństwa odpowiadające co najmniej standardowi wymaganemu przez przepisy o ochronie danych osobowych; postanowienia niniejszej sekcji należy w takim przypadku interpretować w sposób spójny z tymi przepisami. Zastosowanie przez którąkolwiek ze Stron surowszych wewnętrznych środków bezpieczeństwa pozostaje dopuszczalne i nie ogranicza obowiązków wynikających z Umowy. [1] [16]

PODSTAWA PRAWNA
Kodeks cywilny (k.c.) · Ustawa o zwalczaniu nieuczciwej konkurencji (UZNK) · orz. I AGa 336/22 (Sąd Apelacyjny) · RODO (rozp. 2016/679)

§ 5

Zwrot, usunięcie, zniszczenie informacji i nośników

1. Na żądanie Strony Ujawniającej, a także niezwłocznie po zakończeniu współpracy, definitywnym zakończeniu negocjacji albo rezygnacji z dalszych rozmów lub projektu, Strona Otrzymująca zwróci, trwale usunie albo zniszczy — zgodnie z wyborem Strony Ujawniającej — wszelkie Informacje Poufne oraz wszelkie Nośniki je zawierające, niezwłocznie, nie później niż w terminie 7 dni roboczych, z uwzględnieniem zasad należytego wykonania zobowiązań i swobody umów [1].

2. Obowiązek, o którym mowa w ust. 1, obejmuje w szczególności: dokumenty, korespondencję, notatki, wyciągi, analizy, zestawienia, wydruki, kopie robocze, skany, zdjęcia, pliki elektroniczne, wiadomości e-mail, dane przechowywane w komunikatorach, repozytoriach kodu, systemach ticketowych, narzędziach projektowych, środowiskach testowych i deweloperskich, na stacjach roboczych, urządzeniach mobilnych, nośnikach wymiennych oraz w innych systemach lub usługach wykorzystywanych przez Stronę Otrzymującą lub osoby, za które ponosi ona odpowiedzialność [1].

3. Jeżeli Strona Ujawniająca zażąda zwrotu, Strona Otrzymująca wyda materiały i Nośniki w stanie niepogorszonym, z wyłączeniem zwykłego zużycia. Jeżeli Strona Ujawniająca zażąda usunięcia albo zniszczenia, Strona Otrzymująca dokona tego w sposób uniemożliwiający dalsze odczytanie, odtworzenie lub operacyjne wykorzystanie Informacji Poufnych [1] [8].

4. Niezależnie od ust. 1-3 Strona Otrzymująca może zachować wyłącznie jedną kopię Informacji Poufnych w minimalnym, niezbędnym zakresie, jedynie dla celów dowodowych, compliance,

audytu wewnętrznego albo wykonania bezwzględnie obowiązujących przepisów prawa. Taka kopia nie może być wykorzystywana operacyjnie, biznesowo ani ujawniana osobom nieuprawnionym, podlega co najmniej równoważnym zabezpieczeniom jak w okresie współpracy oraz pozostaje objęta wszystkimi obowiązkami poufności wynikającymi z Umowy [1] [8].

5. Jeżeli natychmiastowe usunięcie Informacji Poufnych z kopii zapasowych, archiwów systemowych, logów technicznych albo nośników objętych automatycznym cyklem retencji jest technicznie niewykonalne lub wymagałoby niewspółmiernych działań, Strona Otrzymująca może pozostawić takie dane wyłącznie w zakresie wynikającym z technicznych ograniczeń danego systemu, pod warunkiem że: 1) dane te nie będą przywracane do bieżącego obrotu ani wykorzystywane operacyjnie, chyba że będzie to konieczne do odtworzenia systemu po awarii, 2) dostęp do nich będzie ściśle ograniczony do osób administrujących systemem lub wykonujących obowiązki prawne, 3) pozostaną objęte poufnością, 4) zostaną usunięte lub nadpisane w zwykłym cyklu retencji właściwym dla danego systemu [1] [8].

6. Strona Otrzymująca zapewni wykonanie obowiązków z niniejszej sekcji również przez swoich pracowników, współpracowników, podwykonawców, doradców oraz dostawców usług IT, którym udostępniła Informacje Poufne zgodnie z Umową, i ponosi odpowiedzialność za brak zwrotu, usunięcia albo zniszczenia materiałów pozostających w ich dyspozycji [1] [8].

7. Na żądanie Strony Ujawniającej Strona Otrzymująca przekaże, w formie pisemnej albo elektronicznej, oświadczenie o wykonaniu obowiązków określonych w niniejszej sekcji, ze wskazaniem ewentualnych materiałów zachowanych zgodnie z ust. 4 oraz danych pozostających czasowo w backupach lub archiwach zgodnie z ust. 5. Oświadczenie zostanie przekazane niezwłocznie, nie później niż w terminie 3 dni roboczych od dnia wykonania obowiązku [1].

PODSTAWA PRAWNA
Kodeks cywilny (k.c.) · Ustawa o zwalczaniu nieuczciwej konkurencji (UZNK)

§ 6

Czas obowiązywania, odpowiedzialność i kara umowna

1. Umowa wchodzi w życie z dniem jej podpisania przez obie Strony i zostaje zawarta na czas nieokreślony. Każda ze Stron może wypowiedzieć Umowę z zachowaniem 30-dniowego okresu wypowiedzenia, ze skutkiem na koniec miesiąca kalendarzowego. Umowa obejmuje również Informacje Poufne ujawnione drugiej Stronie przed dniem jej zawarcia w związku z negocjacjami, przygotowaniem lub planowaną współpracą, jeżeli zostały przekazane z zastrzeżeniem poufności albo ich poufny charakter wynikał z okoliczności ujawnienia [1].

2. Rozwiązanie, wygaśnięcie albo wypowiedzenie Umowy, bez względu na przyczynę, nie wpływa na obowiązek zachowania poufności w odniesieniu do Informacji Poufnych ujawnionych w okresie obowiązywania Umowy. W odniesieniu do Informacji Poufnych niestanowiących tajemnicy

przedsiębiorstwa obowiązek poufności trwa przez 5 lat od dnia zakończenia obowiązywania Umowy lub zakończenia współpracy Stron, w zależności od tego, które z tych zdarzeń nastąpi później. W odniesieniu do informacji stanowiących tajemnicę przedsiębiorstwa obowiązek poufności trwa bezterminowo, nie krócej jednak niż do czasu utraty przez te informacje cech tajemnicy przedsiębiorstwa [8] [24].

3. W razie naruszenia obowiązku poufności przez Stronę otrzymującą albo przez osoby, za które ponosi ona odpowiedzialność, Strona ujawniająca jest uprawniona do żądania kary umownej w wysokości 50 000,00 zł (słownie: pięćdziesiąt tysięcy złotych) za każde odrębne naruszenie [1] [24]. Za odrębne naruszenie uważa się w szczególności każde nieuprawnione: 1) ujawnienie, przekazanie lub udostępnienie Informacji Poufnych osobie trzeciej, 2) wykorzystanie Informacji Poufnych poza celem określonym w Umowie, 3) skopiowanie, pobranie, wyeksportowanie albo inne utrwalenie Informacji Poufnych z naruszeniem Umowy, jeżeli prowadzi to do utraty kontroli nad poufnością albo do użycia sprzecznego z Umową. Wielokrotne czynności dotyczące tego samego zdarzenia i tego samego zbioru Informacji Poufnych uważa się za jedno odrębne naruszenie.

4. Zapłata kary umownej nie wyłącza ani nie ogranicza prawa Strony ujawniającej do dochodzenia odszkodowania przewyższającego wysokość zastrzeżonej kary umownej, na zasadach ogólnych, jeżeli poniesiona szkoda przewyższa wysokość tej kary [1].

5. Niezależnie od prawa do dochodzenia kary umownej i odszkodowania, Strona ujawniająca może żądać niezwłocznego zaniechania naruszeń oraz usunięcia ich skutków, w szczególności przez zwrot, trwałe usunięcie albo zniszczenie wszelkich nośników, kopii, backupów, wyciągów i zapisów zawierających Informacje Poufne, a także przez przekazanie pisemnego potwierdzenia wykonania tych czynności [8] [24].

6. Strony potwierdzają, że wysokość kary umownej określona w ust. 3 jest uzasadniona wartością gospodarczą oraz wrażliwością Informacji Poufnych typowych dla projektów IT, w tym dotyczących kodu źródłowego, architektury systemów, dokumentacji, danych klientów, warunków handlowych i know-how [24].

PODSTAWA PRAWNA
Kodeks cywilny (k.c.) · Ustawa o zwalczaniu nieuczciwej konkurencji (UZNK) · Praktyka kontraktowa NDA B2B (PL)

§ 7

Tajemnica przedsiębiorstwa, dane osobowe i postanowienia końcowe

1. Strony potwierdzają, że „Informacje Poufne" w rozumieniu niniejszej Umowy są pojęciem umownym, a w zakresie, w jakim spełniają przesłanki ustawowe, mogą jednocześnie stanowić tajemnicę przedsiębiorstwa. Żadne postanowienie Umowy nie wyłącza ani nie ogranicza ochrony przewidzianej w przepisach powszechnie obowiązujących ani uprawnień Strony dotkniętej naruszeniem do dochodzenia roszczeń ustawowych niezależnie od środków przewidzianych w Umowie [8] [33].

2. Jeżeli w związku z negocjacjami, wdrożeniem albo realizacją współpracy dojdzie do sytuacji, w której jedna ze Stron będzie przetwarzać dane osobowe w imieniu drugiej Strony, Strony przed rozpoczęciem takiego przetwarzania zawrą odrębną umowę powierzenia przetwarzania danych osobowych albo odpowiedni aneks spełniający wymagania prawa właściwego [34]. Do czasu zawarcia takiego dokumentu przekazanie danych osobowych do przetwarzania w imieniu drugiej Strony jest niedopuszczalne [34].

3. O ile Strony wyraźnie nie postanowią inaczej w odrębnym dokumencie, każda ze Stron pozostaje samodzielnie odpowiedzialna za zgodność własnego przetwarzania danych osobowych z przepisami prawa, a niniejsza Umowa sama przez się nie stanowi podstawy do powierzenia przetwarzania danych osobowych [34].

4. Umowa podlega prawu polskiemu [1] [34].

5. Wszelkie spory wynikające z Umowy lub z nią związane będą rozstrzygane przez sąd powszechny właściwy miejscowo dla [wskazanej przez Strony miejscowości albo siedziby oznaczonej Strony], jako sąd wyłącznie właściwy; jeżeli Strony nie uzupełnią tego oznaczenia przy podpisaniu Umowy, zastosowanie mają przepisy powszechnie obowiązujące [1] [34].

6. Zmiana Umowy wymaga co najmniej formy dokumentowej, chyba że dotyczy: zakresu obowiązku poufności, czasu jego trwania, zasad odpowiedzialności, kary umownej, przetwarzania danych osobowych, prawa właściwego albo właściwości sądu; w takim przypadku wymagana jest forma pisemna pod rygorem nieważności [1] [34].

7. Wszelkie zawiadomienia, wezwania i oświadczenia związane z Umową powinny być kierowane na adresy korespondencyjne oraz adresy poczty elektronicznej wskazane przez Strony w Umowie albo w późniejszym zawiadomieniu dokonanym w wymaganej formie. Strona, która zmienia swoje dane do doręczeń, zobowiązana jest niezwłocznie poinformować o tym drugą Stronę; w przeciwnym razie doręczenie dokonane na ostatnio wskazane dane uważa się za skuteczne [1] [34].

8. Oświadczenie lub zawiadomienie składane w związku z Umową uważa się za złożone z chwilą, w której dotarło do drugiej Strony w sposób umożliwiający jej zapoznanie się z jego treścią, w tym także za pośrednictwem poczty elektronicznej na uzgodniony adres [1]. Bieżąca komunikacja robocza Stron, w szczególności projektowa lub techniczna, nie stanowi zmiany Umowy, chyba że spełnia

wymagania określone w ust. 6 [1] [34].

PODSTAWA PRAWNA
Kodeks cywilny (k.c.) · Ustawa o zwalczaniu nieuczciwej konkurencji (UZNK) · RODO (rozp. 2016/679)

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

STRONA A	STRONA B
[pełna firma / imię i nazwisko]	[pełna firma / imię i nazwisko]
_____	_____
[imię i nazwisko reprezentanta]	[imię i nazwisko reprezentanta]
[stanowisko / funkcja]	[stanowisko / funkcja]
Data: _____	Data: _____
Miejsce: _____	Miejsce: _____

Bibliografia i źródła

Wszystkie cytowania [1] – [34] w treści wzorca odpowiadają poniższym pozycjom. Pogrupowane wg typu źródła: przepisy prawa, orzeczenia, praktyka i doktryna.

Przepis prawa · 5 pozycji

1 **Kodeks cywilny (k.c.)**

Dz.U. DU/2025/1071

Art. 353[1]. Strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego.

2 **Kodeks cywilny (k.c.)**

Dz.U. DU/2025/1071

Art. 72[1]. § 1. Jeżeli w toku negocjacji strona udostępniła informacje z zastrzeżeniem poufności, druga strona jest obowią- zana do nieujawniania i nieprzekazywania ich innym osobom oraz do niewykorzystywania tych informacji dla własnych celów, chyba że strony uzgodniły inaczej. § 2. W razie niewykonania lub nienależytego wykonania obowiązków, o których mowa w § 1, uprawniony może żądać od drugiej strony naprawienia szkody albo wydania uzyskanych przez nią korzyści. DZIAŁ III Forma czynności prawnych § 1. Jeżeli w toku negocjacji strona udostępniła informacje z zastrzeżeniem poufności, druga strona jest obowią- zana do nieujawniania i nieprzekazywania ich innym osobom oraz do niewykorzystywania tych informacji dla własnych celów, chyba że strony uzgodniły inaczej. § 2. W razie niewykonania lub nienależytego wykonania obowiązków, o których mowa w § 1, uprawniony może żądać od drugiej strony naprawienia szkody albo wydania uzyskanych przez nią korzyści. DZIAŁ III Forma czynności prawnych

3 **Kodeks cywilny (k.c.)**

Dz.U. DU/2025/1071

Art. 38. Osoba prawna działa przez swoje organy w sposób przewidziany w ustawie i w opartym na niej statucie.

4 **Kodeks cywilny (k.c.)**

Dz.U. DU/2025/1071

Art. 43[1]. Przedsiębiorcą jest osoba fizyczna, osoba prawna i jednostka organizacyjna, o której mowa w art. 331 § 1, prowadząca we własnym imieniu działalność gospodarczą lub zawodową.

8 **Ustawa o zwalczaniu nieuczciwej konkurencji (UZNK)**

Dz.U. DU/2022/1233

Art. 11. 1. Czynem nieuczciwej konkurencji jest ujawnienie, wykorzystanie lub pozyskanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa. Przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ichelementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępnedla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytejstaranności, działania w celu utrzymania ich w poufności. Pozyskanie informacji stanowiących tajemnicę przedsiębiorstwa stanowi czyn nieuczciwej konkurencji, w szczególności gdy następuje bez zgody uprawnionego do korzystania z informacji lub rozporządzania nimi i wynika z nieuprawnionegodostępu, przywłaszczenia, kopiowania dokumentów, przedmiotów, materiałów, substancji, plików elektronicznych obejmujących te informacje lub umożliwiających wnioskowanie o ich treści.

Wykorzystanie lub ujawnienie informacji stanowiących tajemnicę przedsiębiorstwa stanowi czyn nieuczciwej konkurencji, w szczególności gdy następuje bez zgody uprawnionego do korzystania z informacji lub rozporządzania nimi i naruszaobowiązek ograniczenia ich wykorzystywania lub ujawniania wynikający z ustawy, czynności prawnej lub z innego aktualbo gdy zostało dokonane przez osobę, która pozyskała te informacje, dokonując czynu nieuczciwej konkurencji. Ujawnienie, wykorzystanie lub pozyskanie informacji stanowiących tajemnicę przedsiębiorstwa stanowi czyn nieuczciwej konkurencji także wówczas, gdy w chwili ich ujawnienia, wykorzystania lub pozyskania osoba wiedziała lub przyzachowaniu należytej staranności mogła wiedzieć, że informacje zostały pozyskane bezpośrednio lub pośrednio od tego, ktowykorzystał lub ujawnił je w okolicznościach określonych w ust. 4. Wykorzystywanie informacji stanowiących tajemnicę przedsiębiorstwa polegające na produkowaniu, oferowaniu, wprowadzaniu do obrotu, a także przywozie, wywozie i przechowywaniu w tych celach towarów stanowi czyn nieuczciwejkonkurencji, jeżeli osoba dokonująca wskazanej czynności wiedziała lub przy zachowaniu należytej staranności mogła wiedzieć o tym, że właściwości towarów, w tym estetyczne lub funkcjonalne, proces ich wytwarzania lub zbywania zostaływ znacznym stopniu ukształtowane w następstwie czynu określonego w ust. 1, dokonanego w okolicznościach określonychw ust. 4.

Pozyskanie informacji stanowiących tajemnicę przedsiębiorstwa nie stanowi czynu nieuczciwej konkurencji, jeżelinastąpiło w wyniku niezależnego odkrycia lub wytworzenia albo obserwacji, badania, rozłożenia na części, testowaniaprzedmiotu dostępnego publicznie lub posiadanego zgodnie z prawem przez osobę, która pozyskała informacje i którejuprawnienie do pozyskania informacji nie było ograniczone w chwili ich pozyskania. Ujawnienie, wykorzystanie lub pozyskanie informacji stanowiących tajemnicę przedsiębiorstwa nie stanowi czynunieuczciwej konkurencji, gdy nastąpiło w celu ochrony uzasadnionego interesu chronionego prawem, w ramach korzystaniaze swobody wypowiedzi lub w celu ujawnienia nieprawidłowości, uchybienia, działania z naruszeniem prawa dla ochronyinteresu publicznego, lub gdy ujawnienie informacji stanowiących tajemnicę przedsiębiorstwa wobec przedstawicieli pracowników w związku z pełnieniem przez nich funkcji na podstawie przepisów prawa było niezbędne dla prawidłowego wykonywania tych funkcji.

Orzeczenie · 1 pozycja

10 **I AGa 336/22 · Sąd Apelacyjny**

Data: 23.11.2023

W kontekście ochrony tajemnicy przedsiębiorstwa, sąd podkreślił, że wykorzystywanie poufnych informacji przekazanych w ramach współpracy do celów konkurencyjnych stanowi naruszenie umowy oraz przepisów dotyczących nieuczciwej konkurencji. Uprawnione jest dostosowanie zasad korzystania z informacji poufnych, tak aby ich użycie ograniczone było wyłącznie do celu, dla którego zostały udostępnione, co zabezpiecza interesy podmiotu, który te informacje przekazał.

TREŚĆ ORZECZENIA

W praktyce przedsiębiorcy powinni: 1) zawierać umowy NDA, które wyraźnie określają zakres i cel wykorzystania informacji poufnych, 2) ustalać jasne zasady dotyczące ochrony tajemnicy przedsiębiorstwa, w tym sankcje za ich naruszenie, 3) przeprowadzać szkolenia dla pracowników oraz współpracowników na temat tajemnicy przedsiębiorstwa, a także skutków jej bezprawnego wykorzystania,

4) monitorować sposób wykorzystania udostępnionych informacji, żeby mieć pewność, że są one wykorzystywane zgodnie z ...

↗ https://www.saos.org.pl/judgments/495060

Praktyka i doktryna · 6 pozycji

9

Badanie: Polska praktyka umowna NDA: definicja informacji poufnych w projektach IT, czy brak oznaczenia informacji jako poufnej wyłącza ochronę, typowe wyłączenia publicznie znane wcześniej posiadane niezależnie opracowane legalnie pozyskane od osoby trzeciej ujawnienie na żądanie organu. Uwzględnij art. 11 UZNK i swobodę umów.

W polskiej praktyce kontraktowej w projektach IT **definicja „Informacji Poufnych" jest kształtowana swobodnie (art. 353¹ k.c.)**, ale niemal zawsze obejmuje szeroki katalog informacji technicznych, biznesowych i organizacyjnych, z typowymi **wyłączeniami (carve-outs)**: informacje publicznie znane, już posiadane, uzyskane legalnie od osób trzecich, samodzielnie opracowane oraz ujawniane na żądanie organu. Brak oznaczenia informacji jako „poufnej" *nie wyłącza z mocy prawa* ochrony z art. 11 ustawy o zwalczaniu nieuczciwej konkurencji, ale w praktyce – jeśli NDA tego wymaga – może utrudnić objęcie danej informacji kontraktową ochroną i dowód naruszenia. Poniżej usystematyzowane odpowiedzi pod kątem polskiego prawa i praktyki NDA w IT.

1. Podstawa prawna ochrony – art. 11 UZNK + swoboda umów **Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji** (u.z.n.k.):

- art. 11 ust. 1: czynem nieuczciwej konkurencji jest m.in. ujawnienie, wykorzystanie lub pozyskanie cudzych informacji stanowiących **tajemnicę przedsiębiorstwa**.[5][6]

- art. 11 ust. 2: tajemnica przedsiębiorstwa to informacje:

- **techniczne, technologiczne, organizacyjne przedsiębiorstwa** albo inne mające **wartość gospodarczą**,

- które jako całość lub w szczególnym zestawieniu nie są powszechnie znane ani łatwo dostępne dla osób zwykle zajmujących się tym rodzajem informacji,

- **o ile uprawniony przy zachowaniu należytej staranności podjął działania w celu utrzymania ich w poufności**.[4][5][6] Z punktu widzenia prawa cywilnego:

- art. 353[1] Kodeksu cywilnego: strony mogą ułożyć stosunek prawny według swego uznania, byle treść/cel nie sprzeciwiały się ustawie, naturze stosunku ani zasadom współżycia społecznego.[6]

- NDA nie jest typizowana w przepisach; doktryna i praktyka traktują ją jako **umowę nienazwaną**, opartą na art. 353[1] k.c.[4][5][6] W konsekwencji:

- **minimalny poziom ochrony** zapewnia zawsze art. 11 u.z.n.k. (tajemnica przedsiębiorstwa), o ile spełnione są przesłanki materialne i formalne.

- **NDA może tę ochronę: rozszerzać, doprecyzowywać lub organizować (np. definicja informacji poufnych, procedury, kary umowne)**.[4][5][6]

2. Przesłanka „poufności" w rozumieniu art. 11 UZNK Z orzecznictwa i doktryny (cytowanej w opracowaniach praktyków):

- Dwie przesłanki:

- **formalna** – przedsiębiorca musi wykazać, że **podjął działania w celu zachowania poufności**; poufność musi być wyraźnie lub dorozumianie zamanifestowana (np. NDA, procedury, oznaczenia, ograniczenie dostępu).[6] - **materialna** – informacja musi mieć charakter techniczny/technologiczny/organizacyjny lub inną wartość gospodarczą, a jej ujawnienie może obiektywnie negatywnie wpływać na sytuację przedsiębiorcy.[6] Z tego wynika dla praktyki NDA w IT:

- brak oznaczenia „poufne" **nie przekreśla z automatu** możliwości uznania informacji za tajemnicę przedsiębiorstwa, jeżeli są inne przejawy dbałości o poufność (NDA, dostęp „need to know", polityki, logowanie dostępu).[6]

- jednak **ciężar dowodu** leży po stronie ujawniającego – musi wykazać, że konkretne informacje spełniają przesłankę poufności i że podjął środki ochrony.[6]

3. Definicja „Informacji Poufnych" w polskich NDA w IT Z praktyki opisanej przez kancelarie i poradniki:

- Kluczowy element NDA to **precyzyjna definicja „Informacji Poufnych"** – „serce umowy".[7][1][5]

- Umowa zwykle:

- wymienia **kategorie**: informacje techniczne (specyfikacje systemu, kod źródłowy, architektura, API, algorytmy), biznesowe (modele biznesowe, roadmapy produktu), organizacyjne (procedury, know-how), finansowe, dane klientów itd.[1][3][4][6]

- odwołuje się do definicji tajemnicy przedsiębiorstwa z art. 11 u.z.n.k., ale **wykracza poza nią** – obejmuje także informacje, które nie muszą spełniać wszystkich kryteriów tajemnicy przedsiębiorstwa, o ile strony tak postanowią (swoboda umów).[4][5][6]

- często obejmuje **wszelkie informacje ujawnione w związku z projektem**, niezależnie od nośnika (ustnie, pisemnie, w formie elektronicznej, dostępu do systemu, repozytorium kodu). Przykładowo, w komentarzach praktyków podkreśla się, że im **dokładniej określone** informacje poufne, tym łatwiej udowodnić naruszenie.[1][7]

4. Czy brak oznaczenia informacji jako „poufnej" wyłącza ochronę? Trzeba odróżnić dwie płaszczyzny:

4.1. Ochrona ustawowa – art. 11 UZNK

- Ochrona tajemnicy przedsiębiorstwa **nie jest uzależniona wyłącznie** od formalnego oznaczenia informacji jako „poufne".

- Istotne jest, czy przedsiębiorca **podjął działania dla zachowania poufności** (może to być m.in. NDA, ograniczenie dostępu, procedury bezpieczeństwa, ogólna praktyka oznaczania, ale także dorozumiane wymogi poufności).[6]

- Brak oznaczenia może jednak **utrudnić wykazanie** spełnienia przesłanki formalnej, zwłaszcza gdy odbiorca będzie twierdził, że nie wiedział o poufnym charakterze danych.

4.2. Ochrona kontraktowa – typowe NDA W praktyce redakcyjnej są dwa modele: 1. **Model „all information":**

- Informacjami Poufnymi są wszystkie informacje przekazane w związku z projektem, *niezależnie od oznaczenia*, z typowymi wyłączeniami (publiczne itp.).

- Oznaczenie jako „poufne" bywa pomocnicze, ale niekonieczne.

- W takim modelu **brak oznaczenia sam w sobie nie wyłącza ochrony**, choć może osłabiać dowodowo twierdzenie, że druga strona powinna była rozumieć poufny charakter informacji.

2. **Model „oznaczone lub potwierdzone"** (częsty w kontraktach z podmiotami zagranicznymi, korporacjami):

- Informacjami Poufnymi są tylko:

- informacje **opatrzone oznaczeniem**, lub

- informacje ujawnione ustnie, ale w określonym terminie **potwierdzone na piśmie jako poufne**.

- W takim modelu **brak oznaczenia lub potwierdzenia może kontraktowo wyłączyć ochronę** – odbiorca może zasadnie powoływać się na literalne brzmienie umowy. Z uwagi na **swobodę umów** (art. 353^1 k.c.) strony mogą przyjąć dowolne z powyższych rozwiązań, byle nie naruszało to ustawy czy natury stosunku.[6] Dla praktyki IT (w szczególności przy kodzie źródłowym, architekturze, dokumentacji technicznej) częstszy jest model z **domyślną poufnością wszystkich informacji** ujawnionych w ramach projektu, właśnie po to, by nie uzależniać ochrony od formalnego oznaczenia każdej paczki danych.

5. Typowe „carve-outs" w polskich NDA (w tym w IT) Profesjonalna umowa NDA w Polsce „zawsze zawiera tzw. **carve-outs**" – wyłączenia z obowiązku poufności.[3] Typowo wskazuje się, że informacjami poufnymi **nie są** informacje, które:

- są lub staną się **publicznie dostępne**, bez naruszenia NDA przez stronę otrzymującą informacje;[3]

- strona otrzymująca **posiadała już wcześniej** zgodnie z prawem, przed ujawnieniem na podstawie NDA, i może to wykazać (np. własne know-how, wcześniejsze rozwiązania);[3]

- zostały **legalnie uzyskane od osoby trzeciej**, która była uprawniona do ich ujawnienia (nie naruszała własnych zobowiązań poufności);[3]

- zostały **niezależnie opracowane** przez stronę otrzymującą, bez korzystania z informacji poufnych drugiej strony (często wymaga się możliwości udowodnienia tego – np. logi repozytorium, wcześniejsze koncepcje);

- których ujawnienie jest wymagane na podstawie **bezwzględnie obowiązujących przepisów prawa** lub **orzeczeń/żądań właściwych organów lub sądów** – pod warunkiem, że ujawnienie ogranicza się do niezbędnego zakresu, a ujawniający organowi poinformuje drugą stronę, jeśli prawo na to pozwala.[2][3][4] Wyłączenia te są standardem w polskiej praktyce NDA, również opisanej przez PARP i kancelarie.[2][3][4]

6. Ujawnienie na żądanie organu W praktyce klauzule przewidują:

- Strona może ujawnić informację poufną, jeśli jest do tego **zobowiązana przepisami prawa** albo wiążącą decyzją/żądaniem sądu, prokuratury, organu nadzoru itp.[2][3]

- Zwykle nakłada się obowiązki:

- **ograniczenia zakresu ujawnienia** do minimum wymaganego prawem;

- **niezwłocznego poinformowania** drugiej strony o żądaniu, jeśli nie jest to zabronione (np. tajemnica śledztwa);

- współdziałania w celu ograniczenia ujawnienia (np. wnioskowanie o niejawność posiedzenia, anonimizację). Takie ujawnienie **co do zasady nie jest traktowane jako naruszenie NDA**, ale dobrze, by umowa to wprost przesądzała.[2][3]

7. Specyfika projektów IT a definicja informacji poufnych W projektach IT, z perspektywy art. 11 u.z.n.k. i NDA, typowe kategorie informacji:

- **Techniczne / technologiczne**:

- architektura systemu, diagramy, specyfikacje API, konfiguracje infrastruktury, rozwiązania chmurowe, dokumentacja bezpieczeństwa, testy penetracyjne – zwykle stanowią tajemnicę przedsiębiorstwa, jeśli spełnione są przesłanki z art. 11.[4][6]

- kod źródłowy, algorytmy, skrypty CI/CD, konfiguracje systemów monitoringu.

- **Organizacyjne**:

- procesy DevOps, procedury zarządzania incydentami, wewnętrzne standardy kodowania, metodyki wdrożeń.

- **Biznesowe / gospodarcze**:

- roadmapy produktowe, plany wdrożeń, dane o klientach, dane sprzedażowe, modele taryfowe.[4][5][6] Definicja w NDA zwykle obejmuje wszystkie powyższe, niekiedy z dodatkowym wskazaniem, że informacjami poufnymi są także **„wyniki testów, prototypy, PoC, backlog, user stories, dane testowe"** itd.

8. Praktyczne wnioski (na tle art. 11 UZNK i swobody umów)

1. **Warto powiązać definicję z art. 11 u.z.n.k., ale ją rozszerzyć.**

- Dobrą praktyką jest wprowadzenie definicji obejmującej wszystko, co może stanowić tajemnicę przedsiębiorstwa w rozumieniu art. 11 u.z.n.k., oraz dodatkowo inne informacje o zastrzeżonej poufności, nawet jeśli nie spełniają wszystkich ustawowych kryteriów (np. informacje tylko organizacyjne o niewielkiej wartości ale wrażliwe dla stron).[4][5][6]

2. **Brak oznaczenia jako „poufne" nie musi wyłączać ochrony – zależy od redakcji NDA.** - Jeśli definicja obejmuje wszystkie informacje przekazane w związku z projektem, oznaczenie jest jedynie dodatkowym wzmocnieniem dowodowym.

- Jeśli definicja ogranicza się do informacji wyraźnie „oznaczonych", brak oznaczenia może być kontraktowo kluczowy.

3. **Z punktu widzenia art. 11 u.z.n.k. zalecane są mechanizmy manifestowania poufności:**

- NDA, wewnętrzne procedury, oznaczenia dokumentów, ograniczenie dostępu, rejestry udostępnienia, klauzule w umowach z pracownikami i podwykonawcami – wszystko to ułatwia wykazanie spełnienia przesłanki formalnej („działania w celu utrzymania poufności") w razie sporu.[6]

4. **Carve-outs są standardem i z reguły obejmują:**

- publicznie znane, wcześniej posiadane, niezależnie opracowane, legalnie uzyskane od osób trzecich oraz ujawnienie na żądanie organu – dokładnie tak, jak wskazałeś.[2][3][4] Jeżeli chcesz, mogę zaproponować przykładową, „rynkową" definicję Informacji Poufnych i listę wyłączeń, dostosowaną konkretnie do relacji: zamawiający–software house/outsourcing IT.

↗ https://kpaplegal.pl/blog/nda-umowa-o-zachowaniu-poufnosci/

↗ https://www.parp.gov.pl/component/content/article/57196:non-disclosure-agreement-nda

↗ https://mklegal.eu/umowa-nda-co-powinna-zawierac-i-czy-warto-ja-zawrzec/

↗ https://finea.pl/porady-biznesowe/nda-umowa-o-zachowaniu-poufnosci-jakie-elementy-powinna-zawierac/

↗ https://kancelaria-szczurek.pl/czym-jest-umowa-o-zachowaniu-poufnosci-nda/

12

Badanie: Polska NDA B2B tajemnica przedsiębiorstwa klauzula celu ujawnienia informacji poufnych ograniczenie wykorzystania tylko do oceny negocjacji realizacji współpracy zakaz użycia konkurencyjnego brak domniemanej licencji lub przeniesienia IP przez ujawnienie informacji poufnych najlepsze praktyki i orzecznictwo

W relacji **B2B** NDA powinno przede wszystkim: **precyzyjnie zdefiniować informacje poufne**, **ograniczyć ich użycie wyłącznie do wskazanego celu** (np. oceny negocjacji i/lub realizacji współpracy), **zakazać wykorzystania konkurencyjnego**, oraz **wyraźnie wyłączyć jakiekolwiek domniemanie licencji, przeniesienia praw własności intelektualnej albo udzielenia jakichkolwiek praw do IP przez samo ujawnienie informacji**.[2][3][5][8] W polskim prawie rdzeniem ochrony jest **art. 11 ust. 2 ustawy z 16 kwietnia 1993 r.

o zwalczaniu nieuczciwej konkurencji**, zgodnie z którym tajemnicą przedsiębiorstwa są informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawie i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne, *o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął przy zachowaniu należytej staranności działania w celu utrzymania ich w poufności*.[1][7][9] Ustawa penalizuje i deliktowo ujmuje nie tylko** ujawnienie**, ale też** wykorzystanie **i** pozyskanie **tajemnicy przedsiębiorstwa w sposób bezprawny.[8] Najlepsza praktyka przy klauzuli celu to zapis, że odbiorca może używać informacji wyłącznie** do oceny, przygotowania i realizacji konkretnej współpracy **albo** do jednego, ściśle opisanego projektu**, a wszelkie inne użycie jest zakazane.[2][3][5][10] W praktyce warto dodać, że obejmuje to także zakaz wykorzystywania informacji do tworzenia ofert dla podmiotów konkurencyjnych, analiz konkurencyjnych, reverse engineeringu, obejścia ujawniającego lub pozyskiwania przewagi rynkowej poza uzgodnionym celem; taki zakaz mieści się w standardowym rozumieniu „niewykorzystywania poza ustalonym celem" i ochrony tajemnicy przedsiębiorstwa.[3][5][8] Dobrze skonstruowana NDA powinna także obejmować:

- **definicję informacji poufnych** z listą kategorii, dokumentów i danych, najlepiej z objęciem także kopii, opracowań i wersji pochodnych,[2][3][6]

- **wyłączenia**, np. informacje publiczne, legalnie znane wcześniej odbiorcy, otrzymane od osoby trzeciej bez obowiązku poufności, niezależnie opracowane bez użycia informacji poufnych,[10]

- **obowiązki organizacyjne**: ograniczenie dostępu do osób „need to know", zabezpieczenie techniczne, zakaz kopiowania poza potrzebę projektu, zwrot lub zniszczenie nośników po zakończeniu współpracy,[2][3]

- **czas trwania poufności**, przy czym w odniesieniu do tajemnicy przedsiębiorstwa często stosuje się okres „tak długo, jak informacja zachowuje przymiot poufności i wartość gospodarczą", a dla części kontraktowej można dodać termin określony lub bezterminowy w granicach dopuszczalnych przez charakter informacji.[6][9] Co do **braku domniemanej licencji / przeniesienia IP**, w NDA warto wpisać wyraźnie, że:

- ujawnienie informacji poufnych **nie przenosi żadnych autorskich praw majątkowych**, praw do baz danych, know-how ani innych praw własności intelektualnej,

- nie udziela **żadnej licencji**, z wyjątkiem wprost i pisemnie określonej licencji lub sublicencji,

- wszelkie prawa do rezultatów prac, utworów, wynalazków i usprawnień wymagają odrębnej umowy. To jest szczególnie ważne w B2B, bo sama klauzula poufności reguluje *dostęp i użycie informacji*, a nie automatycznie *własność IP*; źródła praktyczne wyraźnie podkreślają, że NDA służy ochronie informacji, nie zastępuje umowy licencyjnej ani cesji praw.[1][3][4][6] Jeśli chodzi o **orzecznictwo**, istotne jest stanowisko, że ochrona tajemnicy przedsiębiorstwa zależy od spełnienia przesłanek ustawowych, w tym od realnych działań ochronnych i wartości gospodarczej informacji; w przywołanych materiałach wskazano m.in. na orzeczenia **NSA z 21 września 2021 r., III OSK 596/21** oraz **NSA z 17 marca 2016 r., I OSK 2740/15**, podkreślające znaczenie ekonomicznej wartości informacji i uprzedniego zastrzeżenia poufności wobec konkretnych danych.[9] To wspiera praktykę, by NDA nie była ogólnikowa, lecz odnosiła się do konkretnych kategorii informacji, celu i środków ochrony.[2][3][5][10] W doktrynie i praktyce kancelaryjnej najczęściej rekomenduje się więc model: **celowość + ograniczenie wykorzystania + zakaz konkurencyjnego użycia + brak licencji/przeniesienia IP + ścisłe wyłączenia + obowiązek zwrotu/zniszczenia**.[2][3][5][10] Jeśli chcesz, mogę przygotować od razu **propozycję konkretnej klauzuli po polsku** do umowy B2B, z wersją „krótką” i „rozszerzoną”, uwzględniającą tajemnicę przedsiębiorstwa, zakaz użycia konkurencyjnego oraz zastrzeżenie braku licencji/IP.

↗ https://kancelaria-walawski.pl/tajemnica-przedsiebiorstwa-i-zakaz-konkurencji-w-modelu-b2b/

↗ https://www.kkz.com.pl/2025/09/03/tajemnica-przedsiebiorstwa-i-klauzule-poufnosci-jak-skutecznie-chro

↗ https://tajemnica-przedsiebiorstwa.pl/nda/

↗ https://www.fakturaxl.pl/nda-umowa-o-zachowaniu-poufnosci

↗ http://lipinskiwalczak.pl/nk/ogolne/czym-jest-klauzula-poufnosci/

16

Badanie: RODO art. 5 ust. 1 lit. f i art. 32 jako podstawa kontraktowych wymogów bezpieczeństwa w NDA B2B IT: need-to-know, MFA, szyfrowanie, logi, zgłaszanie incydentów

RODO **dopuszcza** oparcie szczegółowych wymogów bezpieczeństwa w NDA/B2B IT (need-to-know, MFA, szyfrowanie, logi, zgłaszanie incydentów) na art. **5 ust. 1 lit. f** oraz art. **32** rozporządzenia 2016/679, o ile środki te są wynikiem analizy ryzyka i są „odpowiednie” do tego ryzyka.

1. Podstawa normatywna – dlaczego można to „oprzeć na RODO”

1. **Art. 5 ust. 1 lit. f RODO – zasada integralności i poufności** Art. 5 ust. 1 lit. f rozporządzenia 2016/679 („RODO”) nakazuje, aby dane osobowe były przetwarzane „w sposób zapewniający **odpowiednie bezpieczeństwo** danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą **odpowiednich środków technicznych lub organizacyjnych**”.[5] Zasada integralności i poufności jest więc ogólną normą, która „domaga się” konkretyzacji w postaci środków bezpieczeństwa (polityki, procedury, wymagania kontraktowe).[1][5]

2. **Art. 32 RODO – konkretyzacja wymogu bezpieczeństwa** Art. 32 ust. 1 RODO zobowiązuje administratora **i podmiot przetwarzający** do wdrożenia „odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku”, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób.[2][8] Przepis przykładowo (katalog otwarty) wymienia m.in.:

- **pseudonimizację i szyfrowanie danych osobowych** (art. 32 ust. 1 lit. a),[2]

- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (lit. b),[2]

- zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu (lit. c),[2] - regularne testowanie, mierzenie i ocenę skuteczności środków (lit. d).[2]

3. **Powiązanie art. 5 i 32** Wytyczne EROD (np. Wytyczne 05/2021) wskazują, że ryzyko dla praw i wolności osób należy uwzględniać przy wdrażaniu środków na podstawie m.in. art. **5** i art. **32** RODO.[4] To uzasadnia użycie tych przepisów jako podstawy do budowania **konkretnych obowiązków kontraktowych** wobec partnera B2B, który faktycznie przetwarza dane.

4. **Umowa jako narzędzie realizacji obowiązków z RODO**

- Art. 28 ust. 1 RODO nakazuje administratorowi korzystać wyłącznie z podmiotów przetwarzających, które dają „**wystarczające gwarancje**" wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób.[6]

- W praktyce doktryna i UODO wskazują, że weryfikacja i wymogi wobec dostawcy IT obejmują m.in. szyfrowanie, uwierzytelnianie wieloskładnikowe, backupy, procedury awaryjne, logowanie zdarzeń.[3][6] NDA / umowa B2B IT jest zatem naturalnym miejscem, by „przełożyć" art. 5 i 32 na język **konkretnych wymagań technicznych i organizacyjnych**.

2. Jak „podpiąć" konkretne mechanizmy pod art. 5 ust. 1 lit. f i art. 32 Poniżej, dla każdego z wymienionych przez Ciebie środków, wskazanie, jak go **uzasadnić** w świetle RODO i orzecznictwa/praktyki.

2.1. Zasada „need-to-know" / ograniczenie dostępu

- Wynika bezpośrednio z wymogu zapewnienia **poufności** (art. 5 ust. 1 lit. f, art. 32 ust. 1).[5][2]

- Zgodnie z art. 32, środki mają zapewnić m.in. poufność i integralność systemów i usług przetwarzania.[2]

- W praktycznych wytycznych dla art. 32 wskazuje się jako standard:

- „ograniczenie dostępu do danych tylko do osób uprawnionych" – jako podstawowy środek bezpieczeństwa dla małych i średnich firm.[3]

- W umowach/ankietach wstępnych administratorzy rutynowo wymagają od dostawcy informacji o **zarządzaniu uprawnieniami** i organizacji dostępu.[3][6] **Kontraktowo** można więc zapisać: – że strona zapewni dostęp do danych jedynie osobom działającym z upoważnienia, w zakresie koniecznym do realizacji umowy (konkretyzacja „need-to-know"), – że będzie stosować cykliczny przegląd uprawnień i procedurę nadawania/odbierania dostępów. Można powołać jako podstawę art. 5 ust. 1 lit. f i art. 32 ust. 1 RODO.

2.2. MFA / uwierzytelnianie wieloskładnikowe

- Art. 32 nie wymienia MFA z nazwy, ale wymaga środków „odpowiednich do ryzyka", z uwzględnieniem stanu wiedzy technicznej.[2][8] - W opracowaniach praktycznych dotyczących art. 32 uwierzytelnianie dwuskładnikowe jest wskazywane jako **standardowy środek** dla zapewnienia bezpieczeństwa systemów IT, w szczególności poczty i dostępu do systemów z danymi osobowymi.[3][6]

- Przykładowo, jako rekomendację dla małych i średnich firm podaje się: „**silne hasła i uwierzytelnianie dwuskładnikowe**".[3]

- UODO w decyzjach, w których stwierdza naruszenie art. 32, zwraca uwagę na **brak adekwatnych środków uwierzytelniania** i kontroli dostępu jako naruszenie art. 5 ust. 1 lit. f i art. 32.[7] **Kontraktowo:** – można żądać stosowania MFA przynajmniej dla: dostępów administratorów, zdalnych połączeń, paneli zarządzania usługą, skrzynek e-mail, przez które przechodzą dane osobowe. Uzasadnienie: art. 32 ust. 1 RODO w zw. z art. 5 ust. 1 lit. f – adekwatny środek do zminimalizowania ryzyka nieuprawnionego dostępu.

2.3. Szyfrowanie

- Art. 32 ust. 1 lit. a RODO wprost wymienia „**szyfrowanie danych osobowych**" jako przykładowy środek techniczny.[2]

- Motyw 83 RODO podkreśla, że administrator/podmiot przetwarzający powinni oszacować ryzyko i wdrożyć **środki, takie jak szyfrowanie**, minimalizujące to ryzyko, tak by zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność.[2]

- W praktyce art. 32 interpretuje się jako obejmujący szyfrowanie „w spoczynku i w tranzycie" (dane na dyskach, backupach, transmisja, np. TLS).[3] **Kontraktowo** można więc wymagać:

- szyfrowania danych osobowych w transmisji (np. protokoły zapewniające poufność komunikacji),

- szyfrowania nośników (serwery, laptopy, backupy) z danymi osobowymi,

- procedur zarządzania kluczami kryptograficznymi. Bezpośrednia podstawa prawna: art. 32 ust. 1 lit. a w zw. z art. 5 ust. 1 lit. f RODO.

2.4. Logowanie zdarzeń (logi)

- Art. 32 ust. 1 lit. b–d mówi o zdolności do zapewnienia poufności, integralności, dostępności oraz o **regularnym testowaniu, mierzeniu i ocenianiu skuteczności** środków.[2]

- Bez prowadzenia logów dostępu i zdarzeń nie ma praktycznej możliwości:

- wykrywania incydentów,

- weryfikacji, czy środki bezpieczeństwa działają,

- udokumentowania spełniania wymogów art. 32.

- Wytyczne praktyczne do art. 32 wskazują wprost „**zarządzanie dostępami (role, logowanie zdarzeń)**" jako standardowy element środków bezpieczeństwa oraz wykorzystanie narzędzi SIEM/DLP do monitorowania incydentów.[3] **Kontraktowo:** – można wprost nałożyć na partnera obowiązek:

- prowadzenia logów dostępu i operacji na danych osobowych,

- adekwatnego czasu przechowywania logów,

- zabezpieczenia logów przed modyfikacją,

- udostępniania wybranych logów administratorowi na potrzeby audytu czy analizy incydentów. Podstawa: art. 32 ust. 1 lit. b–d RODO (zapewnienie poufności, kontrola i ocena skuteczności środków).

2.5. Zgłaszanie incydentów

- Art. 33 RODO reguluje obowiązek **zgłaszania naruszeń ochrony danych** organowi nadzorczemu przez administratora, a art. 33 ust. 2 nakłada na podmiot przetwarzający obowiązek **„niezwłocznego zgłaszania" administratorowi naruszenia ochrony danych osobowych po jego stwierdzeniu**. To już samodzielna, szczególna podstawa dla obowiązku „incident reporting" w relacji ADO–procesor.

- Art. 32 wiąże się z tym, że systemy bezpieczeństwa muszą umożliwiać w ogóle **wykrycie** naruszeń (co z kolei wymaga logów, monitoringu itp.).[2][3] **Kontraktowo:** – należy:

- powtórzyć obowiązek z art. 33 ust. 2 RODO i doprecyzować terminy (np. godziny, a nie „bez zbędnej zwłoki"),

- rozciągnąć go na „incydenty bezpieczeństwa" w szerszym rozumieniu (nie tylko naruszenia ochrony danych, ale także zdarzenia potencjalnie prowadzące do naruszenia),

- opisać formę, zakres informacji, tryb eskalacji i współpracy w analizie incydentu. Podstawa: art. 33 ust. 2 RODO (obowiązek zgłoszenia naruszenia ADO) w zw. z art. 32 (systemy bezpieczeństwa) i art. 5 ust. 1 lit. f (integralność i poufność).

3. Relacja do NDA / umowy B2B IT – jak to spiąć prawnie

1. **Charakter umowy**

- Jeśli druga strona przetwarza dane osobowe w imieniu administratora – poza NDA konieczna jest **umowa powierzenia** z art. 28 RODO, w której art. 5 ust. 1 lit. f i art. 32 są bezpośrednio relewantne.

- W praktyce wiele podmiotów wprowadza jeden dokument łączący NDA, SLA i postanowienia powierzenia, ale istotne jest wyraźne odróżnienie części wykonującej obowiązki z art. 28 RODO.

2. **Klauzule odwołujące się do RODO** W części dotyczącej bezpieczeństwa można wprost wskazać, że:

- środki wymienione (need-to-know, MFA, szyfrowanie, logi, zgłaszanie incydentów) są wdrażane „w wykonaniu obowiązków wynikających z art. 5 ust. 1 lit. f oraz art. 32 RODO",

- druga strona zapewnia „wystarczające gwarancje" w rozumieniu art. 28 ust. 1 RODO w zakresie wdrożenia i utrzymywania tych środków.[6] 3. **Analiza ryzyka jako „most" między przepisem a konkretnym środkiem**

- Art. 32 ust. 1 opiera wybór środków na **analizie ryzyka**.[2][3]

- W praktyce warto kontraktowo przewidzieć:

- obowiązek dokumentowania analizy ryzyka przez podmiot przetwarzający,

- okresową rewizję środków (odniesienie do „stanu wiedzy technicznej"),

- możliwość żądania aktualnych informacji o środkach bezpieczeństwa (ankiety, raporty, certyfikaty typu ISO/IEC 27001, o którym mowa w art. 32 ust. 3 jako sposobie wykazywania zgodności).[3][2]

4. **Praktyka i orzecznictwo**

- W decyzjach UODO naruszenie art. 32 często jest rozpatrywane łącznie z naruszeniem art. 5 ust. 1 lit. f RODO (niewdrożenie adekwatnych środków bezpieczeństwa oznacza naruszenie zasady integralności i poufności).[7]

- W materiałach praktycznych dotyczących outsourcingu IT podkreśla się konieczność kontraktowego uregulowania m.in. szyfrowania, backupów, szybkiego przywrócenia dostępności danych, stosowania MFA oraz środków organizacyjnych (polityki bezpieczeństwa).[6][3]

4. Wnioski dla konstrukcji klauzul

- **Tak** – można wprost oprzeć kontraktowe wymogi bezpieczeństwa (need-to-know, MFA, szyfrowanie, logi, zgłaszanie incydentów) na art. 5 ust. 1 lit. f oraz art. 32 RODO (plus art. 28 i 33 dla powierzenia i notyfikacji).

- **Warunek** – środki muszą być opisane jako:

- adekwatne do zidentyfikowanego ryzyka,

- odnoszące się do poufności, integralności, dostępności i odporności systemów (słownictwo art. 32),

- podlegające okresowej ocenie i aktualizacji (art. 32 ust. 1 lit. d). Jeśli chcesz, mogę zaproponować konkretne brzmienia klauzul umownych (PL/EN) z odwołaniami do art. 5, 28, 32 i 33 RODO, obejmujących wprost need-to-know, MFA, szyfrowanie, logi i procedurę obsługi incydentów.

↗ https://rkrodo.pl/zasady-przetwarzania-danych-osobowych-art-5-rodo/

↗ https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-32-bezpieczenstwo-przetwarza

↗ https://rpms.pl/praktyczne-zasady-przetwarzania-danych-osobowych-w-sposob-teleinformatyczny-art-32

↗ https://uodo.gov.pl/pl/file/4498

↗ https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-5-zasady-dotyczace-przetwarz

24

Badanie: Polska praktyka kontraktowa NDA B2B IT: okres obowiązywania umowy vs czas trwania obowiązku poufności, kara umowna za każde naruszenie poufności 50 000 zł, możliwość dochodzenia odszkodowania uzupełniającego ponad karę, żądanie zaniechania i usunięcia skutków; aktualny stan prawny 2026

W polskiej praktyce kontraktowej **NDA B2B** warto rozróżniać **okres obowiązywania umowy** od **czasowego zakresu obowiązku poufności**: umowa może obowiązywać tylko w czasie współpracy, a obowiązek poufności może trwać także po jej zakończeniu. Podstawą są przede wszystkim zasady swobody umów i odpowiedzialności kontraktowej z Kodeksu cywilnego, a mechanizmy typu **kara umowna**, **odszkodowanie uzupełniające**, **zaniechanie** i **usunięcie skutków naruszenia** są co do zasady dopuszczalne, ale wymagają precyzyjnego uregulowania w treści NDA.

- **Okres obowiązywania umowy vs. czas trwania poufności**

- W praktyce trzeba odróżnić:

- **czas trwania umowy** – czyli kiedy strony są związane całą umową NDA;

- **czas trwania obowiązku poufności** – czyli jak długo wykonawca ma zachować tajemnicę informacji, także po rozwiązaniu albo wygaśnięciu umowy.

- Takie rozdzielenie jest zgodne z zasadą swobody umów z art. 353^1 Kodeksu cywilnego oraz z konstrukcją zobowiązania, które może obejmować obowiązki trwające po ustaniu samej współpracy.[?]

- **Podstawa prawna odpowiedzialności za naruszenie poufności**

- Naruszenie NDA co do zasady stanowi **niewykonanie albo nienależyte wykonanie zobowiązania**, więc stosuje się art. 471 Kodeksu cywilnego.[?]

- Jeżeli stroną jest przedsiębiorca B2B, odpowiedzialność kontraktowa będzie oceniana według ogólnych reguł prawa cywilnego, a nie prawa pracy.[?]

- **Kara umowna 50 000 zł za każde naruszenie**

- Co do zasady jest to dopuszczalne na podstawie art. 483 § 1 Kodeksu cywilnego, który pozwala zastrzec karę umowną za **niewykonanie lub nienależyte wykonanie zobowiązania niepieniężnego**.[?]

- Obowiązek poufności ma charakter **niepieniężny**, więc może być objęty karą umowną.[?]

- W praktyce trzeba bardzo precyzyjnie opisać, co oznacza **„jedno naruszenie"**, bo przy zbyt ogólnym sformułowaniu powstaje spór, czy kara należy się za każde ujawnienie, każde przekazanie, każdy dzień naruszenia, czy każdą osobę, która uzyskała dostęp.

- Kwota **50 000 zł za każde naruszenie** jest co do zasady dopuszczalna, ale może być później **miarkowana** przez sąd na podstawie art. 484 § 2 Kodeksu cywilnego, jeżeli zobowiązanie zostało w znacznej części wykonane albo kara jest rażąco wygórowana.[?]

- **Odszkodowanie uzupełniające ponad karę**

- To jest możliwe, ale tylko wtedy, gdy NDA wyraźnie to przewiduje.

- Z art. 484 § 1 Kodeksu cywilnego wynika, że w razie zastrzeżenia kary umownej wierzyciel co do zasady nie może żądać odszkodowania ponad karę, **chyba że strony inaczej postanowiły**.[?]

- Dlatego w NDA trzeba dodać klauzulę typu: **„Zapłata kary umownej nie wyłącza prawa dochodzenia odszkodowania przenoszącego jej wysokość na zasadach ogólnych."**

- Bez takiego zastrzeżenia możliwość dochodzenia szkody ponad karę jest ograniczona przez art. 484 § 1 Kodeksu cywilnego.[?] - **Żądanie zaniechania naruszeń**

- Tego rodzaju roszczenie jest co do zasady możliwe jako roszczenie o **niewykonywanie dalszych naruszeń** i o usunięcie skutków naruszenia zobowiązania kontraktowego, zwłaszcza gdy NDA przewiduje taki obowiązek wprost.[?]

- W praktyce zapisuje się to jako:

- obowiązek natychmiastowego zaprzestania ujawniania;

- zakaz dalszego używania informacji;

- obowiązek zwrotu albo trwałego usunięcia nośników, kopii i wyciągów;

- potwierdzenie usunięcia informacji w określonym terminie.

- Jeżeli w relacji pojawi się też **tajemnica przedsiębiorstwa**, podstawą mogą być dodatkowo przepisy ustawy o zwalczaniu nieuczciwej konkurencji, które przewidują roszczenia o zaniechanie, usunięcie skutków i naprawienie szkody.[?]

- **Usunięcie skutków naruszenia**

- W NDA B2B warto wprost wskazać obowiązki typu:

- usunięcie plików;

- zwrot dokumentacji;

- zniszczenie kopii;

- złożenie pisemnego oświadczenia o wykonaniu tych czynności;

- poinformowanie o przekazaniu informacji dalej, jeżeli do tego doszło.

- Taki zapis wzmacnia pozycję dowodową wierzyciela i ułatwia dochodzenie wykonania zobowiązania zgodnie z art. 354 i art. 471 Kodeksu cywilnego.[?]

- **Aktualny stan prawny 2026**

- Na gruncie **Kodeksu cywilnego** powyższe konstrukcje są nadal aktualne w 2026 r.; nie ma ogólnego zakazu kar umownych w NDA B2B ani zakazu zastrzegania poufności po ustaniu umowy.[?]

- W praktyce najważniejsze ryzyka nie wynikają z samej konstrukcji NDA, lecz z:

- nieprecyzyjnego określenia informacji poufnych;

- braku rozróżnienia między okresem umowy a okresem poufności;

- zbyt szerokiej albo zbyt wysokiej kary bez opisu sposobu naliczania;

- braku klauzuli o odszkodowaniu uzupełniającym;

- braku mechanizmu zwrotu/usunięcia materiałów.

- Jeżeli chcesz, mogę od razu przygotować **wzorcową klauzulę NDA B2B po polsku** z: okresem obowiązywania, 50 000 zł kary za każde naruszenie, odszkodowaniem uzupełniającym, zaniechaniem i obowiązkiem usunięcia skutków, w wersji „pro-inwestor" albo „pro-wykonawca". Uwaga: podane wyniki wyszukiwania dotyczą głównie ryzyka **rekwalifikacji B2B na etat** i nie zawierają wiarygodnych źródeł o samej konstrukcji NDA; dlatego oparłem odpowiedź przede wszystkim na ogólnych regułach Kodeksu cywilnego i praktyce kontraktowej, a nie na tych wynikach.

↗ https://latwy-start.pl/pl/transition-to-b2b-in-poland/

↗ https://umowywit.pl/nowe-uprawnienia-pip-a-umowy-b2b/

↗ https://prawodlabiznesu.eu/umowa-b2b-w-it-co-warto-wiedziec/

↗ https://zakaz-konkurencji.pl/ksef-w-2026-dla-programisty-i-freelancera-na-b2b/

↗ https://dudkowiak.pl/blog/reforma-pip-i-ryzyko-zmiany-klasyfikacji-umowy-b2b-2026/

33

Badanie: Polska praktyka kontraktowa B2B mutual NDA w branży IT: relacja NDA do tajemnicy przedsiębiorstwa (art. 11 i 18 UZNK), klauzula o odrębnej umowie powierzenia danych osobowych zgodnej z art. 28 RODO, wybór prawa polskiego, klauzula prorogacyjna sądu właściwego (art. 46 k.p.c.), zmiana umowy w formie dokumentowej/pisemnej oraz zasady zawiadomień i doręczeń. Uwzględnij aktualność na 2026-06-15 i praktyczne ryzyka redakcyjne.

Poniżej masz **praktyczny, polski wzorzec redakcyjny** dla **mutual NDA B2B w IT** z uwzględnieniem relacji do **tajemnicy przedsiębiorstwa** (art. 11 i 18 ustawy o zwalczaniu nieuczciwej konkurencji), **odrębnej umowy powierzenia danych** zgodnej z art. 28 RODO, **prawa polskiego**, **prorogacji sądu** (art. 46 k.p.c.), **zmiany umowy** oraz **zawiadomień i doręczeń**. Uwzględniam też praktyczne ryzyka redakcyjne i stan na **2026-06-15**.

1) NDA a tajemnica przedsiębiorstwa: relacja, której nie wolno mieszać **NDA nie zastępuje reżimu tajemnicy przedsiębiorstwa**. W polskim prawie ochronę tajemnicy przedsiębiorstwa zapewnia przede wszystkim **art. 11 ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji** (dalej: **u.z.n.k.**), a roszczenia cywilne za naruszenie — **art. 18 u.z.n.k.**[1] W praktyce NDA pełni trzy funkcje:

- **doprecyzowuje**, jakie informacje strony uznają za poufne;

- **rozszerza ochronę kontraktową** także na informacje, które nie spełniają jeszcze wszystkich przesłanek „tajemnicy przedsiębiorstwa";

- **organizuje dowodowo** zasady oznaczania, zwrotu, usunięcia i odpowiedzialności. Najbezpieczniej redakcyjnie przyjąć, że:

- **„Informacje poufne"** obejmują szerszy katalog informacji niż ustawowa tajemnica przedsiębiorstwa;

- **„Tajemnica przedsiębiorstwa"** jest tylko jedną z kategorii informacji poufnych, ale nie odwrotnie;

- NDA **nie wyłącza** ustawowej ochrony z u.z.n.k., a jedynie ją uzupełnia.[1] To ważne, bo art. 11 u.z.n.k. chroni informację tylko wtedy, gdy ma ona wartość gospodarczą, nie jest powszechnie znana, a uprawniony podjął przy zachowaniu należytej staranności działania w celu utrzymania jej w poufności.[1] Jeśli w NDA wpiszesz zbyt szeroką definicję bez procedur ochronnych, możesz uzyskać **umowę „na papierze", ale słabą dowodowo**.

Ryzyka redakcyjne

- **Za szeroka definicja** typu „wszelkie informacje ujawnione” bez wyjątków i bez celu ujawnienia.
- **Brak wskazania, że obowiązek poufności dotyczy także materiałów ustnych**, jeśli są potwierdzone później na piśmie/dokumentowo.

- **Brak klauzuli o obowiązku ograniczenia dostępu** tylko do osób „need to know”.

- **Brak rozdzielenia** poufności od ochrony danych osobowych i od tajemnicy przedsiębiorstwa.

- **Automatyczny zakaz wszystkich publikacji referencyjnych** bez mechanizmu uprzedniej zgody, co w IT bywa praktycznie zbyt restrykcyjne i rodzi spory o portfolio.

2) Jak ułożyć definicję informacji poufnych W praktyce warto pisać: > „Informacje Poufne” oznaczają wszelkie informacje ujawnione przez Stronę Ujawniającą drugiej Stronie, w jakiejkolwiek formie, w związku z negocjacjami lub wykonywaniem Umowy, w szczególności dotyczące: kodu źródłowego, architektury systemów, dokumentacji technicznej, roadmap, specyfikacji, testów, bezpieczeństwa, podatności, danych biznesowych, cen, marż, klientów, dostawców, know-how, planów produktowych oraz innych informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu art. 11 u.z.n.k.[1] Dalej dodaj:

- wyjątki: informacje publiczne, legalnie znane wcześniej, legalnie pozyskane od osoby trzeciej, niezależnie opracowane;

- cel wykorzystania: wyłącznie na potrzeby oceny i wykonywania umowy;

- okres ochrony: co najmniej przez czas obowiązywania umowy i po jej ustaniu przez określony czas, a dla tajemnicy przedsiębiorstwa — tak długo, jak zachowuje ten status.[1]

Uwaga praktyczna W IT warto **wyraźnie wymienić**: repozytoria, branch’e, konfiguracje środowisk, dane testowe, logi, tokeny, klucze API, backlog, architecture decision records, raporty bezpieczeństwa i dane dostępu. Bez tego spór często dotyczy tego, czy dany artefakt „był w ogóle informacją poufną”.

3) Sankcje i roszczenia: art. 18 u.z.n.k. oraz kara umowna Art. 18 u.z.n.k. przewiduje roszczenia m.in. o zaniechanie naruszania, usunięcie skutków, złożenie oświadczenia, naprawienie szkody na zasadach ogólnych, wydanie bezpodstawnie uzyskanych korzyści oraz zasądzenie odpowiedniej sumy pieniężnej na cel społeczny.[1] W NDA warto dodać **karę umowną** za naruszenie poufności, ale z dwoma zastrzeżeniami:

- kara umowna dotyczy **zobowiązań niepieniężnych**;

- nie powinna być absurdalnie wysoka, bo wtedy rośnie ryzyko miarkowania przez sąd i sporu o jej realność. Praktycznie bezpieczniej jest zastrzec:

- karę za **każde naruszenie** albo za **każdy przypadek ujawnienia**;

- prawo dochodzenia **odszkodowania uzupełniającego** ponad karę, jeśli szkoda jest wyższa.

4) Odrębna umowa powierzenia danych osobowych: art. 28 RODO Jeżeli w ramach NDA lub współpracy strony przetwarzają **dane osobowe** na rzecz drugiej strony, NDA **nie może zastąpić** umowy powierzenia. Art. 28 ust. 3 RODO wymaga, aby przetwarzanie przez podmiot przetwarzający było uregulowane **umową lub innym instrumentem prawnym** wiążącym administratora z podmiotem przetwarzającym, z określeniem m.in. przedmiotu, czasu trwania, charakteru i celu przetwarzania, rodzaju danych, kategorii osób, obowiązków i praw administratora.[2]

Najważniejsza praktyka W NDA wpisz klauzulę: > „Jeżeli w związku z Umową dojdzie do przetwarzania danych osobowych, Strony zawrą przed rozpoczęciem takiego przetwarzania odrębną umowę powierzenia przetwarzania danych osobowych zgodną z art. 28 RODO; do czasu jej zawarcia Strona nie jest uprawniona do udostępniania drugiej Stronie danych osobowych do przetwarzania w charakterze podmiotu przetwarzającego.” To jest redakcyjnie ważne, bo sama NDA zwykle **nie zawiera wszystkich obligatoryjnych elementów** z art. 28 ust. 3 RODO.[2]

Ryzyka redakcyjne

- mylenie **udostępnienia danych** z **powierzeniem**;

- brak wskazania, która strona jest administratorem, a która procesorem;

- brak rozróżnienia danych klientów, użytkowników, pracowników i kontraktorów;

- zbyt ogólne odesłanie do „zgodności z RODO" bez konkretnych obowiązków;

- wpisanie obowiązku powierzenia „w razie potrzeby" bez zakazu rozpoczęcia przetwarzania przed podpisaniem DPA.

5) Prawo właściwe: wybór prawa polskiego W umowach B2B z elementem zagranicznym można skutecznie wybrać prawo właściwe dla zobowiązań umownych, zgodnie z **rozporządzeniem Rzym I**.[3] W relacjach czysto krajowych po prostu wskazuje się: > „Niniejsza Umowa podlega prawu polskiemu."

Ryzyko redakcyjne Jeżeli kontrahent jest zagraniczny, sam wybór prawa polskiego **nie wyłącza** przepisów bezwzględnie obowiązujących prawa właściwego dla kwestii pozaumownych albo regulacji publicznoprawnych, zwłaszcza w obszarze danych osobowych i prawa pracy. Dla NDA w IT to istotne, bo w tle może pojawić się również ocena, czy współpraca B2B nie ma cech stosunku pracy — a od 2026 r. praktyczne ryzyka kontroli PIP są opisywane jako wyższe w obiegu publicznym i eksperckim.[4][6][7]

6) Prorogacja sądu: art. 46 k.p.c. W sprawach cywilnych strony mogą umownie ustalić sąd właściwy, o ile przepisy nie wyłączają takiej możliwości, zgodnie z **art. 46 § 1 k.p.c.**[5] W praktyce NDA w IT najczęściej stosuje się zapis: > „Sądem wyłącznie właściwym do rozstrzygania sporów wynikłych z niniejszej Umowy będzie sąd powszechny właściwy miejscowo dla siedziby Powoda / pozwanego / siedziby Zamawiającego."

Ryzyka redakcyjne - **Nieprecyzyjne określenie sądu** jako „sąd właściwy dla Warszawy" bez wskazania rodzaju i podstawy właściwości;

- zapis niespójny z przepisami o właściwości wyłącznej;

- wpisanie arbitrażu „przypadkowo", gdy strony nie chcą arbitrażu;

- brak rozróżnienia między sporem o NDA a sporami o dane osobowe czy prawa własności intelektualnej. W praktyce bezpieczne są dwie wersje:

- **sąd właściwy dla siedziby powoda** — bardziej elastyczny, ale mniej przewidywalny;

- **sąd właściwy dla siedziby pozwanego / Zamawiającego** — częsty w B2B, ale negocjacyjnie bardziej „silny" dla jednej strony.

7) Zmiana umowy: dokumentowa czy pisemna W polskiej praktyce najczęściej stosuje się wymóg **formy dokumentowej** albo **pisemnej pod rygorem nieważności** dla zmian umowy. Z perspektywy prawa cywilnego forma dokumentowa jest szersza i obejmuje nośnik umożliwiający ustalenie osoby składającej oświadczenie; pisemna jest surowsza.[6]

Co jest praktycznie lepsze w NDA B2B IT

- jeśli umowa jest „żywa" i zmieniana operacyjnie, lepsza bywa **forma dokumentowa** dla zmian, aneksów technicznych, listy osób uprawnionych, kanałów kontaktu, adresów doręczeń;

- jeśli chcesz większej dyscypliny kontraktowej, możesz zastrzec, że **istotne zmiany** wymagają formy pisemnej, a mniej istotne — dokumentowej.

Ryzyka redakcyjne

- klauzula „zmiany wymagają formy pisemnej" bez doprecyzowania, czy chodzi o **rygor nieważności**, czy tylko cel dowodowy;

- brak zgodności z praktyką podpisu elektronicznego i obiegu skanów;

- konflikt między „tylko pisemnie” a faktycznym uzgadnianiem zmian mailem przez zespoły projektowe. Najbezpieczniejszy zapis operacyjny: > „Zmiana Umowy wymaga formy dokumentowej, chyba że Strony zastrzegły dla danej zmiany formę pisemną pod rygorem nieważności.” To pozwala uniknąć sytuacji, w której każda drobna aktualizacja wymaga formalnego aneksu podpisywanego kwalifikowanym podpisem albo własnoręcznie.

8) Zawiadomienia i doręczenia W NDA warto rozdzielić:

- **adresy do doręczeń umownych**;

- **adresy e-mail do zawiadomień operacyjnych**;

- regułę skuteczności doręczenia;

- obowiązek aktualizacji danych kontaktowych. ### Przykładowa konstrukcja > „Wszelkie zawiadomienia związane z Umową będą składane na adresy wskazane w komparycji Umowy lub na inne adresy uprzednio wskazane drugiej Stronie w formie dokumentowej. Zawiadomienia e-mail uważa się za skutecznie doręczone w dniu wysłania na wskazany adres, o ile nadawca nie otrzymał komunikatu o niedostarczeniu wiadomości.”

Ryzyka redakcyjne

- utożsamianie wysłania e-maila z doręczeniem bez zastrzeżenia, co dzieje się przy błędzie skrzynki;

- brak obowiązku aktualizacji adresu;

- brak wskazania, że zmiana danych kontaktowych jest skuteczna dopiero po powiadomieniu;

- mieszanie doręczeń umownych z doręczeniami procesowymi — to drugie regulują przepisy postępowania, a nie sama umowa. W praktyce warto dodać, że **zmiana adresu do doręczeń wymaga zawiadomienia drugiej strony**, a do czasu takiego zawiadomienia doręczenie na dotychczasowy adres uznaje się za skuteczne.

9) Minimalny zestaw klauzul, który powinien znaleźć się w mutual NDA IT

- definicja informacji poufnych;

- wyjątki od poufności;

- cel użycia informacji;

- obowiązek zachowania poufności przez pracowników i współpracowników;

- zakaz inżynierii wstecznej, kopiowania, publikacji i benchmarków bez zgody;

- zasady oznaczania materiałów i potwierdzania informacji ustnych;

- zwrot/usunięcie danych po zakończeniu współpracy;

- kara umowna i odszkodowanie uzupełniające;

- odrębna umowa powierzenia danych osobowych zgodna z art. 28 RODO;

- prawo polskie;

- prorogacja sądu na podstawie art. 46 k.p.c.;

- forma zmiany umowy;

- zawiadomienia i doręczenia;

- czas trwania poufności;

- zakaz cesji bez zgody, jeśli strony chcą kontroli nad przekazaniem umowy.

10) Najważniejsze ryzyka praktyczne w 2026 r. W branży IT NDA nie może być projektowane w oderwaniu od szerszego ryzyka B2B. W obiegu eksperckim i branżowym wskazuje się, że od 2026 r. rośnie znaczenie kontroli modeli współpracy B2B i ryzyka ich reklasyfikacji, a także potencjalnych konsekwencji finansowych i administracyjnych.[4][6][7][8][10] To nie zmienia samej logiki NDA, ale oznacza, że umowa powinna być spójna z rzeczywistą praktyką współpracy, a nie tylko z formalnym nagłówkiem „B2B". Jeżeli chcesz, mogę w kolejnym kroku przygotować **gotowy, kompletny wzór mutual NDA po polsku** dla IT z tymi klauzulami, w wersji **krótkiej 2–3 strony** albo **rozbudowanej korporacyjnej**.

↗ https://umowywit.pl/jak-przygotowac-firme-it-na-nowe-uprawnienia-pip/

↗ https://lukaszoles.pl/umowa-nda-wzor-dla-firmy/

↗ https://rpms.pl/umowy-b2b-zlecenie-2026-nowe-przepisy-ryzyko-uop/

↗ https://www.youtube.com/watch?v=gleKO-jwV7g

↗ https://zakaz-konkurencji.pl/ksef-w-2026-dla-programisty-i-freelancera-na-b2b/

34

Badanie: Polska praktyka kontraktowa mutual NDA B2B IT: klauzula o odrębnej umowie powierzenia zgodnej z art. 28 RODO, prawo polskie, sąd właściwy, forma dokumentowa zmian, doręczenia e-mail

W polskiej praktyce **mutual NDA B2B IT** można w jednym dokumencie uregulować poufność, ale **klauzula o powierzeniu danych osobowych musi spełniać wymagania art. 28 RODO** i nie może ograniczać się do ogólnego NDA.[1][6][7] Jeśli zakres współpracy obejmuje przetwarzanie danych „w imieniu" drugiej strony, bezpiecznym standardem jest albo odrębna umowa powierzenia, albo wyraźny, kompletny **załącznik/DPA** w umowie głównej.[2][5][6]

- **Klauzula powierzenia** powinna obejmować co najmniej: przedmiot i czas trwania przetwarzania, charakter i cel, rodzaj danych i kategorie osób, obowiązki i prawa administratora oraz obowiązki procesora, w tym poufność osób upoważnionych.[1][5][7]

- EROD wskazuje, że art. 28 RODO wymaga **formy pisemnej, w tym elektronicznej**; niepisana umowa nie spełnia wymogu.[6]

- W praktyce dopuszczalne jest ujęcie powierzenia w **tej samej umowie** co NDA, ale tylko wtedy, gdy część RODO jest dostatecznie precyzyjna i „udokumentowana" zgodnie z art. 28 ust. 3 RODO.[2][6][7] W zakresie wskazanych przez Ciebie klauzul kontraktowych:

- **Prawo polskie**: w umowach B2B standardowo wybiera się prawo polskie na podstawie autonomii kontraktowej z art. 3 rozporządzenia Rzym I, a przy NDA/DPA w relacji między przedsiębiorcami nie ma zwykle przeszkód, by wskazać prawo polskie jako właściwe.[*inference based on general law; no search result directly covered this point*]

- **Sąd właściwy**: w obrocie B2B często wpisuje się sąd właściwy dla siedziby jednej ze stron; klauzula jurysdykcyjna jest dopuszczalna, o ile nie narusza reguł bezwzględnie obowiązujących. W dostarczonym materiale przykład rządowy przewiduje zapis: „**Sądem właściwym dla rozpatrzenia sporów wynikających z Umowy będzie sąd właściwy dla Administratora**".[8]

- **Forma dokumentowa zmian**: dla zmiany NDA/DPA w obrocie profesjonalnym często stosuje się **formę dokumentową** albo co najmniej pisemną, a EROD podkreśla wymóg formy pisemnej/elektronicznej dla samego powierzenia.[6][*inference based on general contract practice; no direct source in results on amendments*]

- **Doręczenia e-mail:** w praktyce kontraktowej doręczenia przez e-mail są często akceptowane jako doręczenia na adresy wskazane w umowie; jednak skuteczność zależy od treści konkretnej klauzuli i od tego, czy strony zastrzegły, że e-mail wywołuje skutek doręczenia.[*inference based on general contract practice; no direct source in results on email notices*] Jeśli chcesz, mogę od razu przygotować **krótki, gotowy wzór klauzul** do mutual NDA B2B IT:

- **RODO / powierzenie**,

- **prawo i sąd właściwy**,

- **zmiany w formie dokumentowej**,

- **doręczenia e-mail.**

↗ https://biz.legalis.pl/dostep-osob-wspolpracujacych-na-podstawie-umow-b2b-do-danych-osobowych-podl

↗ https://zakaz-konkurencji.pl/umowa-o-powierzeniu-danych-rodo-w-b2b-czy-musisz-ja-miec/

↗ https://cab.com.pl/2025/09/23/art-28-rodo-w-praktyce-obowiazki-administratora-danych/

↗ https://bulldogjob.pl/readme/ochrona-danych-osobowych-na-b2b

↗ https://prawodlabiznesu.eu/outsourcing-uslug-it-a-rodo-jak-bezpiecznie-powierzac-dane-osobowe-uslugo

Niniejszy wzorzec został wygenerowany przez UMOWY.AI — system łączący polską bazę 149 000 przepisów prawa, orzecznictwo SAOS oraz aktualną praktykę kontraktową. Każda generacja przechodzi iteracyjną weryfikację jakości (do 2 000 źródeł, do 8 iteracji przeglądu jakościowego). Dokument ma charakter demonstracyjny — nie stanowi porady prawnej. Przed wykorzystaniem we własnym obrocie zaleca się konsultację z prawnikiem.