Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2026/2394

6.11.2026

ZALECENIE KOMISJI (UE) 2026/2394

z dnia 29 października 2026 r.

w sprawie niewiążących modelowych postanowień umownych dotyczących dostępu do danych i ich wykorzystywania oraz niewiążących standardowych postanowień umownych na potrzeby umów o przetwarzanie w chmurze

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

uwzględniając 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 wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) ([1]), w szczególności jego art. 41,

a także mając na uwadze, co następuje:

(1) Sprawiedliwe prawa i obowiązki umowne sprzyjają budowaniu zaufania między uczestnikami rynku i mogą być pomocne w upowszechnianiu sprawiedliwego dostępu do danych i ich wykorzystywania, a także sprzyjają tworzeniu bardziej konkurencyjnego rynku usług przetwarzania danych, umożliwiając tym samym pełne wykorzystanie korzyści płynących z gospodarki opartej na danych w Unii.

(2) Aby zaspokoić potrzeby gospodarki cyfrowej i usunąć bariery stojące na drodze do dobrze prosperującego wewnętrznego rynku danych, rozporządzeniem (UE) 2023/2854 ustanowiono zharmonizowane ramy określające, kto jest uprawniony do wykorzystywania danych z produktu lub z usługi powiązanej, na jakich warunkach i na jakiej podstawie. Głównym narzędziem wykorzystywanym do tego celu w rozporządzeniu (UE) 2023/2854 są umowy. Od czasu rozpoczęcia stosowania tego rozporządzenia wykorzystywanie danych nie opiera się już na faktycznej kontroli nad danymi, lecz na umowach. Ma to na celu zagwarantowanie pewności prawa w odniesieniu do praw i obowiązków stron, a tym samym promowanie dzielenia się danymi. Ponadto rozporządzenie (UE) 2023/2854 ma na celu zapewnienie, za pomocą zrównoważonych umów, sprawiedliwego udziału w korzyściach dla wszystkich stron w łańcuchu wartości danych.

(3) W rozporządzeniu (UE) 2023/2854 przewidziano prawa i obowiązki stron zaangażowanych w proces dostępu do danych i ich wykorzystywania, ustanawiając zasady obowiązkowego dzielenia się danymi, a jednocześnie umożliwiając stronom określenie w umowach praktycznego aspektu wykonywania ich praw i obowiązków w odniesieniu do takiego dostępu do danych i ich wykorzystywania.

(4) Usługi przetwarzania danych są podstawowym czynnikiem umożliwiającym transformację cyfrową i kluczowym czynnikiem konkurencyjności w epoce cyfrowej. Zdolność klienta do zmiany jednej usługi na inną lub do jednoczesnego korzystania z usług kilku dostawców jest kluczowym warunkiem bardziej konkurencyjnego rynku z niższymi barierami wejścia dla nowych dostawców. W rozporządzeniu (UE) 2023/2854 ustanowiono przepisy dotyczące praw klientów do zmiany dostawcy usług przetwarzania danych na innego dostawcę lub na lokalną infrastrukturę oraz określono szczegółowe warunki i procedury, które obejmują również bezpieczeństwo i ciągłość działania podczas procesu zmiany dostawcy. W rozporządzeniu (UE) 2023/2854 uwzględniono również kwestię równoczesnego korzystania z wielu usług przetwarzania danych, co sprzyja skutecznej realizacji strategii wielochmurowych. Ponadto rozporządzenie (UE) 2023/2854 stanowi, że wszystkie strony uczestniczące w procesie zmiany dostawcy muszą współpracować w dobrej wierze.

(5) Prawa i obowiązki klientów i dostawców usług przetwarzania danych są określone w umowach o świadczenie usług przetwarzania danych. Rozporządzeniem (UE) 2023/2854 nałożono na dostawców usług przetwarzania danych obowiązek usuwania przeszkód, które mogłyby utrudniać klientom zmianę dostawcy, w tym przeszkód umownych.

(6) Zgodnie z art. 41 rozporządzenia (UE) 2023/2854 zadaniem Komisji jest opracowanie modelowych postanowień umownych dotyczących dostępu do danych i ich wykorzystywania oraz standardowych postanowień umownych na potrzeby umów o przetwarzanie w chmurze, które posłużą jako narzędzie wspierające strony w negocjowaniu i zawieraniu takich umów oraz propagujące modele zawierające sprawiedliwe, zasadne i niedyskryminujące prawa i obowiązki umowne.

([1]) Dz.U. L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj.

(7) Zgodnie z rozporządzeniem (UE) 2023/2854 głównym celem tych modeli jest pomoc przedsiębiorstwom, w szczególności MŚP, w sporządzaniu, negocjowaniu i zawieraniu takich umów. Rozporządzenie (UE) 2023/2854 stanowi również, że te modelowe postanowienia umowne, jeżeli będą stosowane powszechnie i w całości, powinny mieć korzystny wpływ na kształt umów w sprawie dostępu do danych i ich wykorzystywania, a tym samym prowadzić w szerszym ujęciu do bardziej sprawiedliwych stosunków umownych przy dostępie do danych i dzieleniu się danymi.

(8) Cele te pokazują, że modelowe i standardowe postanowienia umowne powinny odgrywać ważną rolę w stosowaniu rozporządzenia (UE) 2023/2854 oraz w pokazywaniu, w jaki sposób można opracować wyważone umowy, w których stosuje się przepisy rozporządzenia (UE) 2023/2854, w tym również w odniesieniu do stosowania przez sądy ogólnej klauzuli kontroli postanowień pod kątem nieuczciwego charakteru ustanowionej w rozporządzeniu (UE) 2023/2854. Ponadto, jak przewidziano w motywie 55 rozporządzenia (UE) 2023/2854, organy rozstrzygania sporów powinny uwzględniać modelowe postanowienia umowne, aby zapewnić jednolite stosowanie tego rozporządzenia.

(9) Swoboda zawierania umów jest podstawową ideą stosunków między przedsiębiorcami i jako taka jest objęta wolnością prowadzenia działalności gospodarczej na mocy Karty praw podstawowych Unii Europejskiej. Komisja niniejszym udostępnia uczestnikom rynku niewiążące modele stosunków umownych, które – jeżeli strony umowy zdecydują się je stosować – mogą być dostosowywane, co wyjaśniono również w załączniku I wprowadzającym modelowe i standardowe postanowienia umowne. Te postanowienia opracowano przede wszystkim na potrzeby relacji między przedsiębiorcami, z uwzględnieniem rozporządzenia (UE) 2023/2854 i innych przepisów Unii. Podobnie jak w przypadku wszystkich umów, gdy strony nawiązują stosunki umowne związane z danymi, muszą przestrzegać bezwzględnie obowiązujących przepisów prawa Unii, takich jak rozporządzenie (UE) 2023/2854, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([2]) lub bezwzględnie obowiązujące przepisy prawa ochrony konsumentów, a także bezwzględnie obowiązujących przepisów prawa krajowego mających zastosowanie do tej konkretnej umowy.

(10) Nieuczciwe postanowienia umowne mogłyby sprawić, że dostęp do danych lub zmiana dostawców usług przetwarzania danych staną się komercyjnie mniej opłacalne, a czasem nawet ekonomicznie zaporowe.

(11) Rozporządzeniem (UE) 2023/2854 wprowadzono kontrolę pod kątem nieuczciwych postanowień umownych dotyczących dostępu do danych i ich wykorzystywania lub odpowiedzialności i środków ochrony prawnej w przypadku naruszenia lub odstąpienia od obowiązków dotyczących danych, gdy zostały one jednostronnie nałożone przez jedną ze stron w umowach zawieranych między przedsiębiorstwami. Przepisy dotyczące tej kontroli postanowień pod kątem nieuczciwego charakteru uwzględniono również w modelowych postanowieniach umownych oraz standardowych postanowieniach umownych.

(12) Konieczne jest ustanowienie modelowych postanowień umownych na potrzeby kilku umów o dostęp do danych i ich wykorzystywanie objętych zakresem stosowania rozdziałów II, III i IV rozporządzenia (UE) 2023/2854. Pierwszy zalecany wzór umowy reguluje stosunek prawny między użytkownikiem produktu skomunikowanego lub usługi powiązanej, który na mocy rozporządzenia (UE) 2023/2854 jest uprawniony do dostępu do danych i ich wykorzystywania, a posiadaczem danych (załącznik II). Chociaż te modelowe postanowienia umowne można stosować jako odrębną umowę równolegle z innymi umowami – a mianowicie a) umową sprzedaży, najmu, dzierżawy lub leasingu produktu skomunikowanego, b) umową o świadczenie usług powiązanych lub c) każdą umową, której zawarcie jest wymagane na mocy rozporządzenia (UE) 2016/679 – można je również włączyć do umowy całościowej, na przykład obejmującej zakup produktu skomunikowanego. Drugi rodzaj umowy objętej modelowymi postanowieniami umownymi to umowa między użytkownikiem a odbiorcą danych (załącznik III). Trzeci rodzaj umowy objętej modelowymi postanowieniami umownymi to umowa zawierana między posiadaczem danych a odbiorcą danych i dotyczy przypadków, w których na posiadaczu danych spoczywa obowiązek prawny udostępnienia danych osobie trzeciej, taki jak obowiązek udostępnienia danych z produktu skomunikowanego lub usług powiązanych odbiorcy danych wskazanemu przez użytkownika (załącznik IV). Czwarty rodzaj umowy objętej modelowymi postanowieniami umownymi to umowa między przedsiębiorstwami dzielącymi się danymi na zasadzie dobrowolności i podlega kontroli postanowień pod kątem nieuczciwego charakteru na mocy rozporządzenia (UE) 2023/2854 (załącznik V).

(13) Konieczne jest ustanowienie standardowych postanowień umownych, które można włączyć do umów o świadczenie usług przetwarzania danych, aby odzwierciedlić prawa i obowiązki klientów oraz dostawców, w świetle rozdziału VI rozporządzenia (UE) 2023/2854, z uwzględnieniem potrzeby usunięcia przeszkód umownych, które mogłyby utrudniać zmianę dostawcy, oraz potrzeby zapewnienia sprawiedliwych, zasadnych i niedyskryminujących praw i obowiązków umownych (załączniki VI–XII).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(14) Aby ułatwić stosowanie modelowych postanowień umownych i standardowych postanowień umownych, należy dołączyć do nich wytyczne i wyjaśnienia w formie pól informacyjnych. Takie wytyczne i wyjaśnienia mają na celu wsparcie stron przez podanie odesłań do odpowiednich obowiązków prawnych, odniesień między poszczególnymi modelowymi i standardowymi postanowieniami oraz – w razie potrzeby – przez wyjaśnienie konsekwencji wyborów, których strony muszą dokonać, odzwierciedlonych w poszczególnych wariantach danego postanowienia umownego,

ZALECA:

1) aby strony umowy stosowały modelowe postanowienia umowne dotyczące dostępu do danych i ich wykorzystywania określone w załącznikach I–V;

2) aby strony umowy stosowały standardowe postanowienia umowne określone w załącznikach I i VI–XII – na potrzeby umów o przetwarzanie w chmurze;

3) aby państwa członkowskie propagowały stosowanie zalecanych modelowych postanowień umownych oraz standardowych postanowień umownych, w tym za pośrednictwem wyznaczonych przez siebie organów rozstrzygania sporów i właściwych organów przewidzianych w rozporządzeniu (UE) 2023/2854.

Sporządzono w Brukseli dnia 29 października 2026 r.

W imieniu Komisji
Michael McGRATH
Członek Komisji

ZAŁĄCZNIK I

WPROWADZENIE OGÓLNE

1. **Przebieg procedury**

W 2022 r. Komisja ustanowiła grupę ekspertów składającą się z ekspertów powołanych jako osoby występujące we własnym imieniu, aby wspierać Komisję w zapewnianiu uczestnikom rynku praktycznych narzędzi umożliwiających wykonywanie nowych praw i obowiązków zgodnie z rozporządzeniem (UE) 2023/2854 (zwanym dalej aktem w sprawie danych). Eksperci opracowali modelowe postanowienia umowne dotyczące dostępu do danych i ich wykorzystywania oraz standardowe postanowienia umowne dotyczące usług przetwarzania danych. Te modelowe i standardowe postanowienia umowne uwzględniono w sprawozdaniu opublikowanym w kwietniu 2025 r. w rejestrze grupy. Grupę ekspertów wspierała podgrupa składająca się z przedsiębiorstw oraz europejskich i krajowych organizacji biznesowych. Podgrupa przekazywała ekspertom informacje zwrotne w trakcie całego procesu opracowywania modelowych i standardowych postanowień.

Aby dostarczyć ekspertom dodatkowych informacji, służby Komisji zorganizowały nie tylko ukierunkowane konsultacje polegające na testowaniu projektów postanowień z przedsiębiorstwami, które zgłosiły się do tego zadania, ale również dwie rundy konsultacji publicznych (jedną na temat wersji modelowych i standardowych postanowień umownych przygotowanej przez ekspertów, a drugą na temat wersji ostatecznej zawartej w sprawozdaniu grupy ekspertów).

Na podstawie sprawozdania grupy ekspertów oraz uwag otrzymanych w ramach konsultacji publicznych, a także zgodnie z wymogami art. 41 aktu w sprawie danych, Komisja przygotowała modelowe i standardowe postanowienia umowne, które zawarto w załącznikach do niniejszego zalecenia.

Te modelowe i standardowe postanowienia umowne nie są wiążące. Zostały one opracowane w taki sposób, aby strony mogły je dostosować do swoich potrzeb. Strony powinny jednak mieć na uwadze, że modelowe i standardowe postanowienia umowne opracowano w taki sposób, aby były zgodne z prawami i obowiązkami przewidzianymi w akcie w sprawie danych, a także aby były ze sobą spójne. Zawierają one informacje o ich dobrowolnym charakterze oraz porady dla stron dotyczące skutków prawnych wprowadzania zmian. Ponadto organy rozstrzygania sporów wyznaczone na podstawie art. 10 aktu w sprawie danych powinny uwzględniać modelowe i standardowe postanowienia umowne.

Modelowe i standardowe postanowienia umowne opracowano głównie na potrzeby stosunków umownych między przedsiębiorstwami. Można je jednak stosować także w stosunkach między przedsiębiorstwami a konsumentami. W takim przypadku należałoby jednak dodać dodatkowe postanowienia, aby zapewnić zgodność umowy z bezwzględnie obowiązującymi przepisami o ochronie konsumentów (np. prawem do odstąpienia od umowy przez konsumenta w przypadku umów zawieranych przez internet lub na odległość).

Stosowanie tych modelowych i standardowych postanowień umownych nie zwalnia stron z obowiązku zapewnienia zgodności z wszelkimi mającymi zastosowanie bezwzględnie obowiązującymi przepisami prawa Unii lub prawa krajowego. Stosowanie modelowych i standardowych postanowień umownych leży wyłącznie w gestii stron. Komisja nie ponosi odpowiedzialności za żadne skutki wykorzystania tych postanowień.

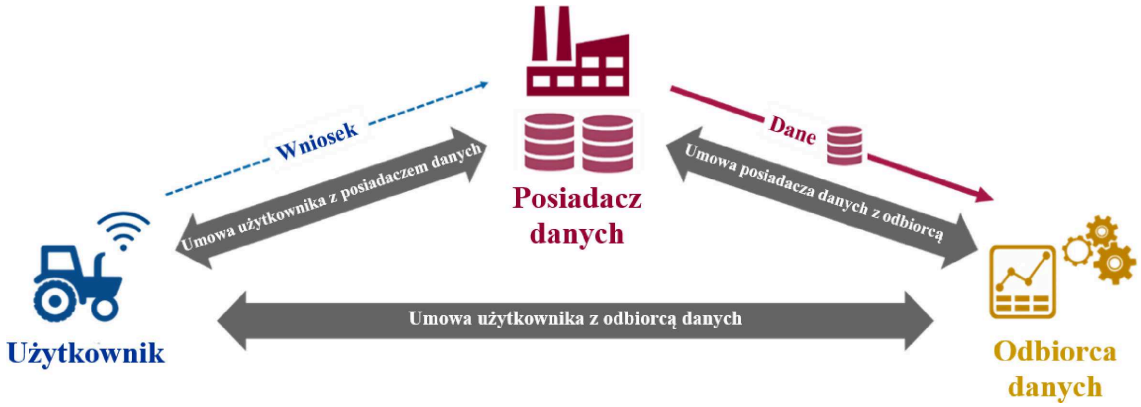
Komisja może dokonać przeglądu tych modelowych i standardowych postanowień umownych w świetle ich stosowania oraz wpływu na przedsiębiorstwa i praktyki rynkowe.

2. **Modelowe postanowienia umowne**

Modelowe postanowienia umowne określone w załącznikach II–V opracowano z myślą o wsparciu stron w sporządzaniu i negocjowaniu umów dotyczących dostępu do danych (osobowych i nieosobowych) i ich wykorzystywania. Umowy te mają na celu zapewnienie sprawiedliwych, zasadnych i niedyskryminujących praw i obowiązków umownych, w tym zasadnej rekompensaty i ochrony tajemnic przedsiębiorstwa.

Strony umowy są określone na początku każdego zestawu modelowych postanowień umownych, w stosownych przypadkach zgodnie z pojęciami zdefiniowanymi w akcie w sprawie danych: dane, posiadacz danych, użytkownik, odbiorca danych itd.

Które modelowe postanowienia umowne należy stosować do poszczególnych rodzajów dzielenia się danymi?



Modelowe postanowienia umowne zawarte w załączniku II opracowano na potrzeby umów między posiadaczem danych a użytkownikiem produktu skomunikowanego lub usługi powiązanej, w przypadku których posiadacz danych zamierza wykorzystywać dane generowane przy użyciu produktu lub usługi.

Modelowe postanowienia umowne zawarte w załączniku III opracowano na potrzeby umów między użytkownikiem produktu skomunikowanego lub usługi powiązanej a odbiorcą danych będącym osobą trzecią, w przypadku gdy użytkownik zwraca się do posiadacza danych z wnioskiem o udostępnienie danych odbiorcy danych na podstawie art. 5 aktu w sprawie danych.

Modelowe postanowienia umowne zawarte w załączniku IV opracowano na potrzeby umów między posiadaczem danych a odbiorcą danych będącym osobą trzecią i przedsiębiorstwem, w przypadku których posiadacz danych jest zobowiązany (na podstawie art. 5 aktu w sprawie danych) do udostępnienia danych odbiorcy na wniosek użytkownika produktu. Można je również stosować z odpowiednimi zmianami, w przypadku gdy posiadacz danych jest zobowiązany do udostępnienia danych odbiorcy danych będącemu osobą trzecią na mocy innych przepisów prawa Unii lub przepisów krajowych przyjętych na podstawie prawa Unii.



Modelowe postanowienia umowne zawarte w załączniku V opracowano na potrzeby umów między osobą dzielącą się danymi a odbiorcą danych, w przypadku których osoba dzieląca się danymi zamierza dobrowolnie udostępnić dane odbiorcy danych, niezależnie od jakiegokolwiek wniosku użytkownika lub podobnej osoby. Termin „osoba dzieląca się danymi" wybrano w celu uwzględnienia wielu możliwych scenariuszy.

Strony powinny określić własną sytuację w odniesieniu do poszczególnych scenariuszy wyjaśnionych powyżej, a następnie zastosować odpowiednie modelowe postanowienia umowne.

Znaczenie prawne modelowych postanowień umownych w odniesieniu do aktu w sprawie danych i innego mającego zastosowanie prawa

Korzystanie z modelowych postanowień umownych przez strony umowy nie wpływa na żadne prawa ani obowiązki stron wynikające z aktu w sprawie danych lub innych przepisów prawa Unii lub prawa państwa członkowskiego przyjętych zgodnie z prawem Unii, w tym na obowiązki administratora i prawa osób, których dane dotyczą, na mocy rozporządzenia (UE) 2016/679 oraz prawa konkurencji.

Strony powinny szczególnie uważać, gdy dzielenie się danymi dotyczy danych osobowych lub mieszanych zbiorów danych. W szczególności posiadacze danych muszą udostępniać dane osobowe użytkownikom lub osobom trzecim, zgodnie z rozporządzeniem (UE) 2023/2854, ale tylko pod warunkiem istnienia podstawy prawnej zgodnie z rozporządzeniem (UE) 2016/679.

Tak jak w przypadku każdej umowy, stosowanie modelowych postanowień umownych przez strony nie wyklucza możliwości uchylenia umowy lub jej poszczególnych postanowień przez właściwy sąd lub jakikolwiek właściwy organ administracyjny z powodu niezgodności z prawem Unii lub prawem państwa członkowskiego.

3. **Standardowe postanowienia umowne**

Standardowe postanowienia umowne mają pomóc stronom we wdrażaniu praw i obowiązków wynikających z aktu w sprawie danych w umowach. Standardowe postanowienia umowne to zestaw klauzul modułowych, które wzajemnie się uzupełniają, ale mogą być również stosowane oddzielnie. Są one przeznaczone do włączania do umów o świadczenie usług przetwarzania danych.

Standardowe postanowienia umowne mają pomóc klientom i dostawcom wszystkich usług przetwarzania danych objętych zakresem stosowania aktu w sprawie danych, niezależnie od tego, czy są to usługi publiczne, prywatne czy inne, małe, średnie czy duże.

Zgodnie z definicją usługi przetwarzania danych zawartą w akcie w sprawie danych te standardowe postanowienia umowne mają zastosowanie do wszystkich modeli usług w chmurze, w tym infrastruktury jako usługi (IaaS), platformy jako usługi (PaaS) i oprogramowania jako usługi (SaaS), jeżeli wykazują one cechy określone w art. 2 ust. 8 aktu w sprawie danych.

Standardowe postanowienia umowne na podstawie aktu w sprawie danych nie obejmują wymogów wynikających z RODO ([1]). Postanowienia umowne zapewniające zgodność z RODO powinny zostać włączone do umowy. Komisja przyjęła standardowe postanowienia umowne dotyczące relacji między administratorem a podmiotem przetwarzającym, aby pomóc zarówno w przestrzeganiu RODO, jak i w przekazywaniu danych osobowych do państw spoza ([2]).

Standardowe postanowienia (klauzule) umowne określone na podstawie RODO umożliwiają podmiotom, które z nich korzystają, zapewnienie i wykazanie zgodności z niektórymi wymogami RODO. Te standardowe postanowienia umowne nie mogą być zmieniane przez strony – mogą zostać włączone do szerszej umowy lub stosowane jako samodzielna umowa.

Jak stosować standardowe postanowienia umowne?

Chociaż zaleca się stosowanie całego zestawu standardowych postanowień umownych, należy zauważyć, że te postanowienia nie stanowią całej umowy o świadczenie usług przetwarzania danych, która obowiązywałaby między klientem a dostawcą. W takiej umowie muszą zostać ujęte dodatkowe zagadnienia, które nie zostały uwzględnione w akcie w sprawie danych ani w standardowych postanowieniach umownych.

Zestaw „definicji" stosowanych w poszczególnych standardowych postanowieniach umownych i dostosowanych do aktu w sprawie danych określono w załączniku XII. W przypadku stosowania definicji innych niż te zaproponowane w standardowych postanowieniach umownych należy odpowiednio dostosować te standardowe postanowienia umowne. Jest to tylko jeden z przykładów dostosowań, które są możliwe przy jednoczesnym wykorzystaniu pełnego zestawu lub części standardowych postanowień umownych.

Dla ułatwienia standardowe postanowienia umowne zawierają odniesienia łączące niektóre postanowienia z odpowiednimi przepisami aktu w sprawie danych lub z innymi standardowymi postanowieniami umownymi.

W określonych sektorach do usług przetwarzania danych mogą mieć zastosowanie dodatkowe przepisy i wymogi, które również należy uwzględnić (np. w sektorach finansowym, zdrowotnym, telekomunikacyjnym, przemysłowym, energetycznym lub publicznym). W akcie w sprawie danych przewidziano wyjątki od niektórych obowiązków dotyczących zmiany dostawcy i odejścia klienta uwzględnionych w standardowych postanowieniach umownych. Dalsze wyjaśnienia można znaleźć w części dotyczącej zmiany dostawcy i odejścia klienta w standardowych postanowieniach umownych.

W akcie w sprawie danych przewidziano konkretne możliwości rozstrzygania sporów:

klient i dostawca mają dostęp do organu rozstrzygania sporów wyznaczonego przez państwa członkowskie zgodnie z art. 10 ust. 4 aktu w sprawie danych oraz

każda ze stron może wnieść skargę do właściwego organu w swoim państwie członkowskim zgodnie z art. 37 ust. 5 lit. b) aktu w sprawie danych.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([2]) Publikacje na temat standardowych postanowień umownych – Komisja Europejska.

W momencie wyznaczania właściwego organu państwa członkowskie określają jego zadania i uprawnienia, które mogą się jednak w pewnym stopniu różnić w poszczególnych państwach członkowskich. Może się zdarzyć, że taki organ nie jest właściwy do rozstrzygania wszystkich sporów między klientem a dostawcą. Strony muszą ocenić najwłaściwszy sposób zobowiązania drugiej strony do wypełnienia jej obowiązków prawnych i zobowiązań umownych oraz sposób rozstrzygania sporów.

Strony mogą uzgodnić objęcie wielu usług jedną umową, którą można nazwać „umową ramową o świadczenie usług" lub inaczej („umowa"). Jest to kolejny powód, dla którego zaleca się dodanie standardowych postanowień umownych do umowy. Jeżeli umowa obejmuje wszystkie usługi, a klient zdecyduje się na zmianę dostawcy w odniesieniu do jednej lub kilku usług, umowa pozostaje w mocy w odniesieniu do pozostałych usług.

Jeżeli strony zamierzają stosować te standardowe postanowienia umowne jedynie częściowo lub wprowadzić do nich zmiany, powinny dokładnie rozważyć, w jaki sposób może to wpłynąć na prawa i obowiązki umowne. W takich sytuacjach zawsze zaleca się skorzystanie z usług doradztwa prawnego lub innego profesjonalnego doradztwa.

ZAŁĄCZNIK II

MODELOWE POSTANOWIENIA UMOWNE

na potrzeby umów o dostęp do danych i ich wykorzystywanie zawieranych między posiadaczami danych a użytkownikami produktów skomunikowanych i usług powiązanych

Modelowe postanowienia umowne mają na celu uregulowanie dostępu do danych i ich wykorzystywania oraz powiązanych kwestii umownych, które mogą powstać między posiadaczem danych a użytkownikami (zgodnie z definicją zawartą w rozporządzeniu (UE) 2023/2854 – zwanym dalej „aktem w sprawie danych").

Główną nowością wprowadzoną przez akt w sprawie danych w tym zakresie jest to, że:

— użytkownikom przyznano prawo dostępu do danych generowanych przez ich produkty skomunikowane lub usługi powiązane (z uwzględnieniem stosowania środków ochrony w odniesieniu do danych chronionych jako tajemnice przedsiębiorstwa);

— użytkownicy mogą również dzielić się danymi z osobami trzecimi, np. w celu korzystania z usług rynku posprzedażowego;

— posiadacz danych musi zawrzeć z użytkownikiem umowę o wykorzystywanie danych nieosobowych i dzielenie się nimi;

— nieuczciwe postanowienia umowne dotyczące dostępu do danych i ich wykorzystywania lub odpowiedzialności i środków ochrony prawnej wobec naruszenia lub odstąpienia od obowiązków dotyczących danych nie są wiążące, jeżeli zostały nałożone na przedsiębiorstwo jednostronnie przez inne przedsiębiorstwo.

Umowa ma strukturę modułową i chociaż może być stosowana jako pełna umowa, strony mogą również wybrać niektóre klauzule odpowiadające ich konkretnej sytuacji. Niektóre postanowienia mogą nie mieć zastosowania do wszystkich produktów i wszystkich umów, na przykład te dotyczące ochrony tajemnic przedsiębiorstwa lub stosowania technicznych środków ochrony. Strony powinny je uwzględnić w umowie wyłącznie w stosownych przypadkach. Podobnie ograniczenia dostępu do danych, ich wykorzystywania lub dzielenia się nimi powinny być uwzględniane w umowach tylko w stosownych przypadkach, tj. gdy w przeciwnym razie zostałyby naruszone wymogi bezpieczeństwa produktu, co mogłoby prowadzić do poważnych negatywnych skutków dla zdrowia, bezpieczeństwa lub ochrony osób fizycznych.

Kilka klauzul zawiera różne warianty, w związku z czym strony powinny przeanalizować swoje szczególne potrzeby, relacje biznesowe i interesy, aby wybrać wariant najlepiej pasujący do ich umowy.

Niektóre klauzule są również opatrzone komentarzem *(w stosownych przypadkach)* i powinny zostać włączone do umowy, jeżeli spełnione są określone warunki.

Mimo że modelowe postanowienia umowne są zalecane przez Komisję, nie są one wiążące i strony mogą zawsze zrezygnować z ich użycia w umowie.

1. Strony oraz produkt/usługi powiązane

1.1. Strony umowy

Niniejsza umowa o dostępie do danych i ich wykorzystywaniu zostaje zawarta

między

(wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia) („posiadacz danych")

Zgodnie z aktem w sprawie danych „posiadacz danych" oznacza „osobę fizyczną lub prawną, która ma prawo lub obowiązek – zgodnie z [aktem w sprawie danych], mającym zastosowanie prawem Unii lub prawem krajowym przyjętym zgodnie z prawem Unii – wykorzystywać i udostępniać dane, w tym, o ile zostało to przewidziane umową, dane z produktu lub dane z usługi powiązanej pobrane lub wygenerowane przez nią podczas świadczenia powiązanej usługi".

W większości scenariuszy posiadaczem danych może być producent produktu lub dostawca odpowiedniej usługi powiązanej lub inna osoba współpracująca z producentem lub dostawcą, która może pobrać dane z produktu lub usługi powiązanej.

Jeżeli jako posiadacz danych może się kwalifikować więcej niż jedna osoba, można to rozwiązać na różne sposoby, na przykład:

a) każda ze stron zawiera własną umowę z użytkownikiem jako niezależny posiadacz danych lub
b) jedna ze stron zawiera umowę z użytkownikiem i w związku z tym działa jako posiadacz danych; w przypadku braku umowy z użytkownikiem pozostałe strony uznaje się za osoby trzecie w rozumieniu klauzuli 3.2. Na podstawie umowy z użytkownikiem i umów z tymi osobami trzecimi posiadacz danych może koordynować dostęp do danych i ich wykorzystywanie.

To, która z tych dwóch możliwości jest preferowana w danym przypadku, zależy od wielu czynników. Strony mogą rozważyć na przykład, czy użytkownicy wolą mieć tylko jednego umawiającego się partnera i jedną umowę. Strony powinny mieć świadomość, że istnieje ścisły związek między wyborem spośród tych dwóch wariantów a sposobem sformułowania przez nie klauzuli 3.2.1.

a

[WARIANT 1] [(*wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia*) („użytkownik")]

[WARIANT 2] [każdą stroną, która identyfikuje się jako użytkownik w rozumieniu aktu w sprawie danych i deklaruje zgodę na warunki niniejszej umowy przez podjęcie następujących kroków: (*wstawić kroki techniczne, jakie musi podjąć każda osoba kwalifikująca się jako użytkownik, takie jak informacje, które należy przekazać, i potwierdzenia, których należy dokonać za pośrednictwem interfejsu użytkownika*) („użytkownik")]

zwanymi w niniejszej umowie łącznie „stronami", a każdy indywidualnie „stroną".

Zgodnie z aktem w sprawie danych „użytkownik" oznacza „osobę fizyczną lub prawną, która jest właścicielem produktu skomunikowanego lub której na podstawie umowy przekazane zostały tymczasowe prawa do korzystania z tego produktu skomunikowanego, lub która korzysta z usług powiązanych". Niniejsza umowa może mieć zastosowanie do szerokiego spektrum scenariuszy. Na jednym krańcu tego spektrum znajdują się scenariusze, w których użytkownik jest znany posiadaczowi danych i w których prawnicy z każdej strony negocjują dostosowaną do konkretnych potrzeb umowę dotyczącą dostępu do danych i ich wykorzystywania (np. linia lotnicza kupująca samoloty od producenta samolotów). Na drugim krańcu znajdują się scenariusze, w których produkty i usługi masowe są wprowadzane na rynek dla milionów konsumentów, którzy nie są indywidualnie znani (a których tożsamość może nawet nie być ujawniana ze względów związanych z ochroną danych), i w których indywidualne negocjacje są po prostu niemożliwe (np. produkty skomunikowane takie jak ekspresy do kawy).

W przypadku scenariuszy tego drugiego rodzaju – oraz wielu innych scenariuszy pośrednich między tymi skrajnościami – pomocne może być identyfikowanie użytkownika nie według nazwy/imienia i nazwiska, lecz na podstawie podjętych kroków (takich jak utworzenie konta użytkownika lub po prostu podłączenie produktu skomunikowanego – np. ekspresu do kawy – oraz zaakceptowanie warunków przez kliknięcie „OK" na wyświetlaczu). Strony powinny mieć świadomość, że – w szczególności w przypadkach dotyczących konsumentów – sądy będą oceniać, czy daną procedurę opracowano w sposób zgodny z przepisami mającego zastosowanie ogólnego prawa zobowiązań i prawa ochrony konsumentów, według tego, jakie warunki muszą być uwzględnione w danej umowie.

1.2. **Produkt/usługi powiązane**

Niniejszą umowę zawiera się w odniesieniu do:

a) następujących produktów skomunikowanych („produkt"): (wstawić nazwę i dalsze specyfikacje konkretnego produktu skomunikowanego lub rodzaju produktów objętych umową);

b) następujących usług powiązanych („usługi powiązane"): (w stosownych przypadkach wstawić nazwę oraz dalsze specyfikacje konkretnych usług powiązanych lub rodzaju usług powiązanych objętych umową).

1.2.1. Użytkownik oświadcza, że jest właścicielem produktu albo jest uprawniony do używania produktu na podstawie umowy najmu, dzierżawy, leasingu lub podobnej umowy lub do otrzymywania usług powiązanych na podstawie umowy o świadczenie usług.

[WARIANT 1] [Użytkownik zobowiązuje się do przekazania posiadaczowi danych, w razie potrzeby, na należycie uzasadniony wniosek, wszelkich istotnych dokumentów na potwierdzenie tych oświadczeń.]

[WARIANT 2] [Dokumentacja potwierdzająca te oświadczenia, a także informacje dotyczące tego, kogo należy uznać za użytkownika na potrzeby niniejszej umowy, zostały określone w **dodatku 9**.]

Zgodnie z aktem w sprawie danych posiadacz danych nie może wymagać od osoby fizycznej ani prawnej dostarczenia jakichkolwiek informacji wykraczających poza to, co jest konieczne do sprawdzenia, czy dana osoba kwalifikuje się jako użytkownik do celów aktu w sprawie danych. W wielu sytuacjach, w szczególności w przypadku towarów powszechnego użytku lub urządzeń biurowych o stosunkowo niskiej wrażliwości generowanych danych (np. ekspresów do kawy, o których mowa powyżej), przeprowadzanie dalszych weryfikacji będzie zazwyczaj nieproporcjonalne.

2. **Dane objęte umową**

Dane objęte niniejszą umową obejmują wszelkie łatwo dostępne dane z produktu lub usług powiązanych w rozumieniu aktu w sprawie danych i obejmują zarówno dane nieosobowe, jak i dane osobowe („dane").

Posiadacz danych wymienia dane w **dodatku 1**, wraz z opisem rodzaju lub charakteru, szacowanej ilości, częstotliwości gromadzenia, miejsca przechowywania i okresu zatrzymywania danych.

Jeżeli w trakcie obowiązywania niniejszej umowy konieczne będzie udostępnienie użytkownikowi danych innych niż określone w dodatku 1, **dodatek 1** zostanie odpowiednio zmieniony.

Zgodnie z aktem w sprawie danych „**dane z produktu**" oznaczają „dane wygenerowane w wyniku korzystania z produktu skomunikowanego, które producent zaprojektował tak, by użytkownik, posiadacz danych lub osoba trzecia, w tym w stosownym przypadku producent, mogli je pobierać za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu".

„**Dane z usług powiązanych**" oznaczają „dane stanowiące cyfrowe odwzorowanie czynności lub zdarzeń z udziałem użytkownika związanych z produktem skomunikowanym, utrwalane przez użytkownika celowo lub generowane jako produkt uboczny jego czynności, podczas świadczenia usługi powiązanej przez dostawcę".

Dane z produktu i usług powiązanych mogą być zarówno danymi osobowymi, jak i nieosobowymi. Obejmują one „dane surowe" oraz „dane, które zostały wstępnie przetworzone, po to aby przed dalszym przetwarzaniem i analizą były zrozumiałe i użyteczne". Nie obejmują natomiast „informacji wywiedzionych lub wywnioskowanych z takich danych, które są wynikiem dodatkowych inwestycji w przypisywanie wartości do danych lub pozyskiwanie wiedzy z danych" (motyw 15).

„**Dane łatwo dostępne**" obejmują „dane z produktu i dane z usługi powiązanej, które posiadacz danych zgodnie z prawem pozyskuje lub może zgodnie z prawem pozyskać z produktu skomunikowanego lub z usługi powiązanej bez nieproporcjonalnie dużego wysiłku wykraczającego poza prostą czynność".

Jak wyjaśniono w motywach, definicja ta nie obejmuje „danych generowanych w wyniku korzystania z produktu skomunikowanego, jeżeli projekt produktu skomunikowanego nie przewiduje przechowywania lub przesyłania takich danych poza elementem składowym, w którym są one generowane, lub poza całym produktem" (motyw 20). „O tym, jakie dane jest w stanie udostępniać produkt skomunikowany, powinny decydować wybory projektowe producenta oraz w stosownym przypadku prawo Unii lub prawo krajowe uwzględniające potrzeby i cele danego sektora lub stosowne decyzje właściwych organów" (motyw 14).

3. **Wykorzystywanie danych i dzielenie się danymi przez posiadacza danych**

3.1. **Uzgodnione wykorzystywanie danych nieosobowych przez posiadacza danych**

3.1.1. Bez uszczerbku dla jakiegokolwiek prawa do wykorzystywania danych posiadacz danych zobowiązuje się wykorzystywać dane nieosobowe wyłącznie do celów uzgodnionych z użytkownikiem, w szczególności do następujących celów:

a) wykonywania umowy z użytkownikiem lub czynności związanych z taką umową (np. wystawiania faktur, sporządzania i dostarczania sprawozdań lub analiz, prognoz finansowych, ocen skutków, obliczania świadczeń dla personelu);

b) zapewniania wsparcia, gwarancji, rękojmi lub podobnych działań lub oceny roszczeń użytkowników, posiadaczy danych lub osób trzecich (np. dotyczących nieprawidłowego działania produktu) związanych z produktem lub usługą powiązaną;

c) monitorowania i utrzymywania funkcjonowania, bezpieczeństwa i ochrony produktu lub usługi powiązanej oraz zapewniania kontroli jakości;

d) poprawy funkcjonowania jakiegokolwiek produktu lub jakiejkolwiek usługi powiązanej oferowanych przez posiadacza danych;

e) opracowywania nowych produktów lub usług przez posiadacza danych, przez osoby trzecie działające w jego imieniu (tj. w przypadku gdy posiadacz danych decyduje, jakie zadania zostaną takim stronom powierzone i odnosi z tego korzyści), we współpracy z innymi stronami lub za pośrednictwem spółek celowych (takich jak spółki *joint venture*);

f) agregacji tych danych z innymi danymi lub tworzenia danych wywnioskowanych w dowolnym zgodnym z prawem celu, w tym w celu sprzedaży lub udostępnienia w inny sposób takich zagregowanych lub wywnioskowanych danych osobom trzecim, pod warunkiem że takie dane nie umożliwiają identyfikacji konkretnych danych przesłanych posiadaczowi danych z produktu skomunikowanego ani nie umożliwiają osobie trzeciej wywnioskowania tych danych ze zbioru danych.

Strony powinny określić cele, w jakich posiadacz danych może wykorzystywać dane nieosobowe, oraz wszystkie szczegóły dotyczące sposobu wykorzystywania tych danych. Strony mogą wybrać cele z katalogu głównych typowych sposobów wykorzystywania danych zaproponowanego w powyższej klauzuli lub dodać własne.

Przy uzgadnianiu wykorzystywania danych strony mogą – w stosownych przypadkach – pogrupować dane w kategorie. Szersze kategorie mogą obejmować w szczególności:

— dane dotyczące statusu produktu lub usługi (np. konfiguracja, wersja, komunikaty diagnostyczne, dane dotyczące zużycia, dane dotyczące konserwacji);

— dane dotyczące sposobu korzystania przez klienta (np. czas aktywności, rodzaje aktywności, geolokalizacja produktu) – należy zauważyć, że dane te mogą w niektórych przypadkach stanowić dane osobowe i wówczas nie są objęte niniejszą klauzulą, lecz klauzulą 3.3 oraz innymi postanowieniami umowy;

— dane dotyczące środowiska użytkownika (np. warunki glebowe, wielkość obszaru);

— ogólne dane środowiskowe (np. dane pogodowe).

Strony powinny mieć świadomość, że domyślne brzmienie podane powyżej w tym zestawie postanowień zakłada, iż cele w nim wymienione są celami realizowanymi przez posiadacza danych będącego stroną tej umowy. Na przykład w odniesieniu do opracowywania nowych produktów lub usług przyjmuje się, że działania rozwojowe są prowadzone przez posiadacza danych, ewentualnie we współpracy z innymi stronami, takimi jak producent komponentów. Dzielenie się danymi z takimi stronami powinno być zatem dozwolone domyślnie, jak przewidziano w klauzuli 3.2.1 lit. a) pkt (i) oraz (ii).

Wykorzystywanie danych do niezależnych celów przez osoby trzecie wymagałoby zawarcia przez te osoby trzecie odrębnej umowy z użytkownikiem albo zastosowania fakultatywnej klauzuli 3.2.1 lit. a) pkt (iii), która zezwala posiadaczowi danych na sprzedaż lub darowiznę danych na rzecz takich osób trzecich do ich własnych celów.

Użytkownik powinien ocenić konsekwencje takiego wykorzystywania danych przez posiadacza danych lub osoby trzecie dla jego własnej działalności i własnych interesów, a w szczególności ocenić, czy powinien otrzymywać wynagrodzenie od posiadacza danych, na przykład w przypadku gdy posiadacz danych może sprzedawać dane generowane przez użytkownika osobom trzecim.

3.1.2. Posiadacz danych zobowiązuje się nie wykorzystywać danych:

a) do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji użytkownika lub na temat korzystania przez użytkownika z produktu lub usługi powiązanej w jakikolwiek inny sposób, który mógłby osłabić pozycję handlową użytkownika na rynkach, na których prowadzi on działalność;

b) [WARIANT] (wskazać sposoby wykorzystywania danych, które na przykład byłyby znacząco szkodliwe dla uzasadnionych interesów użytkownika)].

Strony mogą doprecyzować, jakie rodzaje wykorzystywania danych uznają za na tyle szkodliwe, że należy je wyłączyć. Będzie to zależało od danego sektora i innych okoliczności. W szczególności użytkownik może wyłączyć:

— wykorzystywanie poszczególnych kategorii bardzo wrażliwych danych; lub

— wykorzystywanie danych do określonych celów.

Żadne ze sposobów wykorzystywania danych uzgodnionych w klauzuli 3.1.1 nie mogą być sprzeczne z niniejszą klauzulą, a posiadacz danych zobowiązuje się zapewnić – za pomocą odpowiednich środków umownych, organizacyjnych i technicznych – aby żadna osoba trzecia w ramach organizacji posiadacza danych nie angażowała się w takie wykorzystywanie danych.

3.2. **Dzielenie się danymi nieosobowymi z osobami trzecimi i korzystanie z usług przetwarzania danych**

3.2.1. Bez uszczerbku dla wymogów prawnych wynikających z prawa Unii lub prawa krajowego dotyczących udostępniania danych przez posiadacza danych posiadacz danych może dzielić się z osobami trzecimi danymi będącymi danymi nieosobowymi, jeżeli:

a) dane te są wykorzystywane przez osobę trzecią wyłącznie do następujących celów:

(i) wspierania posiadacza danych w osiąganiu celów dozwolonych na podstawie klauzuli 3.1.1,

(ii) osiągania, we współpracy z posiadaczem danych lub za pośrednictwem spółek celowych, celów dozwolonych na podstawie klauzuli 3.1.1,

(iii) [WARIANT] [(określić cele, do których osoby trzecie mogą dążyć na własne potrzeby, niezależnie od posiadacza danych, oraz czy dzielenie się danymi do tych celów następuje odpłatnie czy nieodpłatnie)] oraz

b) posiadacz danych zobowiązuje osobę trzecią umownie do:

(i) niewykorzystywania danych do jakichkolwiek celów wykraczających poza wykorzystywanie dozwolone zgodnie z klauzulą 3.2.1 lit. a) lub w jakikolwiek sposób wykraczający poza takie wykorzystywanie,

(ii) zachowania zgodności z treścią klauzuli 3.1.2,

(iii) stosowania środków ochrony wymaganych na podstawie klauzuli 3.4.1 oraz

(iv) [WARIANT 1] [niedzielenia się dalej tymi danymi, chyba że użytkownik udzieli ogólnej lub szczególnej zgody na takie dalsze przekazanie. Posiadacz danych musi zobowiązać osobę trzecią, z którą dzieli się danymi, do włączenia klauzul odpowiadających pkt (i)–(iv) do jej umów z odbiorcami.] [WARIANT 2] [niedzielenia się dalej tymi danymi z wyjątkiem przypadków określonych w dodatku 5.]

[WARIANT] [Dalsze szczegółowe informacje, w tym te dotyczące tożsamości lub kategorii osób trzecich, z którymi można dzielić się danymi, ograniczeń w zakresie wykorzystywania danych przez osoby trzecie, a także dalszych warunków i środków ochrony, przedstawiono szczegółowo w **dodatku 5**.]

3.2.2. Niezależnie od klauzuli 3.2.1 posiadacz danych może – na własny rachunek i na własną odpowiedzialność – korzystać z usług przetwarzania danych, np. usług przetwarzania w chmurze (w tym infrastruktury jako usługi, platformy jako usługi i oprogramowania jako usługi), usług hostingu lub podobnych usług w celu osiągnięcia uzgodnionych celów określonych w klauzuli 3.1.1. Osoby trzecie mogą również – na własny rachunek i na własną odpowiedzialność – korzystać z takich usług w celu osiągnięcia uzgodnionych celów określonych w klauzuli 3.2.1 lit. a).

3.3. **Wykorzystywanie danych osobowych i dzielenie się danymi osobowymi przez posiadacza danych**

3.3.1. Posiadacz danych może wykorzystywać, dzielić się z osobami trzecimi lub w inny sposób przetwarzać wszelkie dane będące danymi osobowymi wyłącznie wówczas, gdy istnieje ku temu podstawa prawna, oraz przy spełnieniu warunków dopuszczonych na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([1]) (RODO) oraz – w stosownych przypadkach – dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej).

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

3.4. **Środki ochrony stosowane przez posiadacza danych**

3.4.1. Posiadacz danych zobowiązuje się stosować w celu zapobiegania utracie danych oraz nieuprawnionemu dostępowi do danych środki ochrony, [WARIANT 1] [które są zasadne i odpowiednie w danych okolicznościach, z uwzględnieniem aktualnego stanu wiedzy naukowej i technicznej, potencjalnej szkody dla użytkownika oraz kosztów związanych ze stosowaniem środków ochrony.] [WARIANT 2] [które zostały szczegółowo określone w dodatku 6.]

Strony powinny rozważyć, czy chcą zawrzeć w umowie – w razie potrzeby w oddzielnym dodatku – wszystkie szczegółowe informacje na temat tego, w jaki sposób można skutecznie chronić ważne interesy użytkownika. Środki mogą mieć zarówno charakter techniczny (np. szyfrowanie, zapory sieciowe, przechowywanie danych w odrębnych lokalizacjach), jak i organizacyjny (np. zaangażowanie zaufanej osoby trzeciej). Ponieważ środki muszą być proporcjonalne, ich treść będzie się znacznie różnić w zależności od charakteru danych i wchodzących w grę interesów.

4. **(w stosownych przypadkach) Dostęp użytkownika do danych na wniosek**

Klauzule 4 mają zastosowanie, jeżeli użytkownik nie może uzyskać bezpośredniego dostępu do danych z produktu lub usługi powiązanej zgodnie z art. 3 aktu w sprawie danych. W takim przypadku użytkownik jest uprawniony do uzyskania dostępu do danych od posiadacza danych na wniosek, zgodnie z art. 4 aktu w sprawie danych. Jeżeli użytkownik chce udzielić dostępu do danych odbiorcy danych, zastosowanie mają klauzule 7 poniżej.

4.1. **Obowiązek udostępnienia danych**

4.1.1. Posiadacz danych jest obowiązany udostępnić dane użytkownikowi na wniosek użytkownika lub osoby działającej w jego imieniu wraz z odpowiednimi metadanymi niezbędnymi do interpretacji i wykorzystania tych danych. Wniosek można przekazać za pośrednictwem (*opisać procedurę dotyczącą zwykłego wniosku złożonego drogą elektroniczną, jeżeli jest to technicznie możliwe*). Do celów weryfikacji, czy wniosek został złożony przez użytkownika, posiadacz danych nie wymaga od użytkownika dostarczenia jakichkolwiek informacji poza tymi, które są niezbędne. (*w stosownych przypadkach*) [Jeżeli wniosek składa osoba działająca w imieniu użytkownika, do wniosku załącza się dowód jej umocowania.]

W dodatku 2 przedstawiono szczegółowe informacje, jakie może zawierać wniosek.

4.1.2. Jeżeli użytkownik nie jest osobą, której dane dotyczą, posiadacz danych udostępnia użytkownikowi dane będące danymi osobowymi wyłącznie wówczas, gdy istnieje ważna podstawa prawna udostępnienia danych osobowych zgodnie z art. 6 rozporządzenia (UE) 2016/679 oraz – w stosownych przypadkach – gdy spełnione są warunki określone w art. 9 tego rozporządzenia i art. 5 ust. 3 dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej).

W związku z tym, jeżeli użytkownik nie jest osobą, której dane dotyczą, w każdym wniosku składanym na podstawie poprzedniej klauzuli musi wskazać posiadaczowi danych podstawę prawną przetwarzania zgodnie z art. 6 rozporządzenia (UE) 2016/679 (oraz, w stosownych przypadkach, mające zastosowanie odstępstwo na podstawie art. 9 tego rozporządzenia i art. 5 ust. 3 dyrektywy 2002/58/WE), na której opiera się wniosek o udostępnienie danych osobowych.

4.2. **Charakterystyka danych i ustalenia dotyczące dostępu**

4.2.1. Posiadacz danych jest obowiązany udostępnić dane użytkownikowi, nieodpłatnie dla użytkownika, przy czym dane te muszą cechować się co najmniej taką samą jakością jak w chwili, gdy stały się dostępne dla posiadacza danych, i w każdym wypadku muszą być udostępnione w całościowym, ustrukturyzowanym, powszechnie używanym i nadającym się do odczytu maszynowego formacie.

„Metadane” oznaczają ustrukturyzowany opis treści danych lub sposobu wykorzystywania danych, który ułatwia wyszukiwanie lub wykorzystywanie tych danych. Zgodnie z art. 4 ust. 1 aktu w sprawie danych metadane należy udostępniać wraz z danymi w zakresie, w jakim metadane są „niezbędne do interpretacji i wykorzystania” tych danych.

Chociaż nie określono odpowiednich metadanych potrzebnych do interpretacji i wykorzystania tych danych i w związku z tym trzeba je identyfikować indywidualnie dla każdego przypadku, w akcie w sprawie danych określono, że „[d]ane, które mają być udostępnione, powinny obejmować stosowne metadane, w tym ich podstawowy kontekst i znacznik czasu, aby dane były użyteczne w połączeniu z innymi danymi, takimi jak dane posortowane i sklasyfikowane z innymi odnoszącymi się do nich punktami danych, lub przeformatowane na powszechnie używany format” (motyw 15).

Posiadacz danych i użytkownik mogą korzystać z usług osoby trzeciej (w tym osoby trzeciej świadczącej usługi pośrednictwa danych zdefiniowane w art. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868 ([2])), aby umożliwić użytkownikowi wykonywanie jego praw zgodnie z klauzulą 4.1 niniejszej umowy. Taka osoba trzecia nie będzie uznawana za odbiorcę danych na mocy aktu w sprawie danych, a takie usługi mogą być oferowane przez dostawcę uznawanego za strażnika dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925, chyba że przetwarza on dane do własnych celów biznesowych.

Osoby trzeciej, która świadczy usługę w imieniu posiadacza danych lub użytkownika, nie uznaje się za odbiorcę danych na mocy aktu w sprawie danych, a usługi te mogą być oferowane przez dostawcę uznawanego za strażnika dostępu na podstawie art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 ([3]), chyba że przetwarza on dane do własnych celów biznesowych.

4.2.2. Użytkownikowi należy udzielić dostępu do danych, których dotyczy wniosek:

a) w sposób łatwy i bezpieczny,

b) bez zbędnej zwłoki,

(*w stosownych przypadkach*) [c) w sposób ciągły i w czasie rzeczywistym].

4.2.3. W celu spełnienia wymogów klauzul 4.2.1 i 4.2.2 posiadacz danych określa te ustalenia dotyczące dostępu w dodatku 1.

Zgodnie z art. 4 ust. 1 aktu w sprawie danych dane należy udostępniać bez zbędnej zwłoki oraz, w stosownych przypadkach i jeżeli jest to technicznie wykonalne, w sposób ciągły i w czasie rzeczywistym.

Ponieważ istnieją różne sposoby realizacji tych wymogów prawnych, posiadacz danych powinien określić w dodatku 1 wszystkie szczegółowe informacje dotyczące sposobu udzielania dostępu. Warunki dostępu nie mogą naruszać żadnych praw przyznanych użytkownikowi na mocy aktu w sprawie danych ani innego mającego zastosowanie prawa.

Mając na uwadze to ograniczenie, posiadacz danych powinien w pierwszej kolejności zdecydować, czy chce przewidzieć:

— pełne przekazanie danych, tj. przekazanie kopii danych na nośnik pozostający pod kontrolą użytkownika:

— w drodze transmisji inicjowanej przez posiadacza danych („push"), takiej jak transmisja online, przesłanie do przestrzeni w chmurze użytkownika lub dostarczenie materialnego nośnika, na którym przechowywane są dane, lub

— w drodze pobrania inicjowanego przez użytkownika („pull"), na przykład przez udostępnienie API, dostępu do przestrzeni w chmurze posiadacza danych lub podobnych narzędzi umożliwiających użytkownikowi dostęp do danych i ich wyodrębnienie, lub

— dostęp do danych w miejscu ich przechowywania, tj. dostęp do danych i ich przetwarzanie na nośniku pozostającym pod kontrolą posiadacza danych lub zaufanej osoby trzeciej, na przykład przez zalogowanie się użytkownika do specjalnej przestrzeni na serwerach posiadacza danych lub zaufanej osoby trzeciej, z zastrzeżeniem, że dane nie są przekazywane na nośnik pozostający pod kontrolą użytkownika, chyba że poczyniono szczególne ustalenia w tym względzie.

Pełne przekazanie danych zapewnia użytkownikowi maksymalną swobodę, natomiast dostęp do danych w miejscu ich przechowywania zwiększa ryzyko ujawnienia pomysłów biznesowych użytkowników. Ponadto zgodnie z art. 13 ust. 5 lit. e) aktu w sprawie danych „[d]omniemywa się, że postanowienie umowne jest nieuczciwe do celów ust. 3, jeżeli jego celem lub skutkiem jest […] uniemożliwienie stronie, na którą jednostronnie narzucono postanowienie, uzyskania kopii danych dostarczonych lub wygenerowanych przez tę stronę w okresie obowiązywania umowy lub w rozsądnym okresie po jego rozwiązaniu". W związku z tym zasadę pełnego przekazania danych należy uznać za przepis dyspozytywny.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.U. L 152 z 3.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. L 265 z 12.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

Pełne przekazanie danych w istotnym stopniu ogranicza jednak zdolność posiadacza danych do zapobiegania nadużyciom oraz ochrony jego interesów, np. tajemnic przedsiębiorstwa. Dlatego powinna istnieć również możliwość udzielenia dostępu do danych i ich przetwarzania w miejscu ich przechowywania. Aby pogodzić taki dostęp z interesami użytkownika, często preferowanym rozwiązaniem będzie dostęp do danych przechowywanych na nośniku kontrolowanym przez zaufaną osobę trzecią, a nie przechowywanych na nośniku kontrolowanym przez posiadacza danych. Dostęp do danych w miejscu ich przechowywania powinien co do zasady oznaczać dostęp zdalny, natomiast dostęp na miejscu powinien być ograniczony do sytuacji skrajnych, charakteryzujących się najwyższym stopniem wrażliwości.

W przypadku gdy udziela się dostępu do danych w miejscu ich przechowywania, konieczne jest rozstrzygnięcie szeregu kwestii, w tym zapewnienie, aby pomysły biznesowe użytkownika nie zostały ujawnione, oraz określenie, jakie dane użytkownik może wyodrębnić i przekazać na nośnik pozostający pod jego kontrolą (np. dane wywnioskowane lub dane wywiedzione w wyniku czynności przetwarzania wykonywanych przez użytkownika).

Zgodnie z art. 4 ust. 1 aktu w sprawie danych dane należy udostępniać bez zbędnej zwłoki oraz, w stosownych przypadkach i jeżeli jest to technicznie wykonalne, w sposób ciągły i w czasie rzeczywistym. W związku z tym posiadacz danych powinien określić w dodatku do umowy, czy można udzielić dostępu w sposób ciągły i w czasie rzeczywistym, a jeżeli nie, to z jaką częstotliwością.

Posiadacz danych powinien również rozważyć szereg innych kwestii, takich jak to, jakie dane uwierzytelniające są wymagane, oraz którzy pracownicy użytkownika mogą uzyskać dostęp do danych – i ilu z nich.

4.2.4. Posiadacz danych jest obowiązany przekazać użytkownikowi, bez dodatkowych opłat, informacje niezbędne do uzyskania dostępu do danych zgodnie z art. 4 aktu w sprawie danych.

Obejmuje to w szczególności przekazanie łatwo dostępnych posiadaczowi danych informacji dotyczących wszelkich praw, jakie mogą przysługiwać osobom trzecim w odniesieniu do tych danych, takich jak prawa osób, których dane dotyczą, wynikające z rozporządzenia (UE) 2016/679, lub okoliczności faktycznych, które mogą prowadzić do powstania takich praw.

Posiadacz danych określa te informacje w **dodatku 1**.

Strony zachowują swobodę uzgadniania wszelkiego dodatkowego wsparcia, wykraczającego poza wymogi aktu w sprawie danych, nieodpłatnie lub za opłatą.

4.2.5. Posiadacz danych zobowiązuje się nie przechowywać żadnych informacji na temat dostępu użytkownika do danych, których dotyczy wniosek, poza informacjami, które są niezbędne do:

a) należytego wykonania (i) wniosku użytkownika o dostęp oraz (ii) niniejszej umowy,

b) zapewnienia bezpieczeństwa i utrzymania infrastruktury danych,

c) przestrzegania obowiązków prawnych posiadacza danych w zakresie przechowywania takich informacji.

4.3. **Mechanizm informacji zwrotnej**

Jeżeli użytkownik zidentyfikuje incydent związany z klauzulą 2 – dotyczącą danych objętych umową, z wymogami klauzul 4.2.1 lub 4.2.2 lub z **dodatkiem 1** – dotyczącym charakterystyki danych i ustaleń dotyczących dostępu, oraz jeżeli użytkownik przekaże posiadaczowi danych szczegółowy opis tego incydentu, posiadacz danych i użytkownik muszą współpracować w dobrej wierze w celu zidentyfikowania przyczyny incydentu.

Jeżeli incydent został spowodowany niedopełnieniem obowiązków przez posiadacza danych, posiadacz danych jest zobowiązany usunąć naruszenie bez zbędnej zwłoki. Jeżeli posiadacz danych nie usunie naruszenia, uznaje się to za istotne naruszenie zobowiązania umownego, a użytkownik może powołać się na klauzulę 12 niniejszej umowy. Jeżeli użytkownik uzna, że jego prawo dostępu na mocy art. 4 ust. 1 aktu w sprawie danych zostało naruszone, jest również uprawniony do wniesienia skargi do właściwego organu wyznaczonego zgodnie z art. 37 ust. 5 lit. b) aktu w sprawie danych.

Klauzula ta daje posiadaczowi danych możliwość naprawienia wszelkich naruszeń jego obowiązków prawnych lub zobowiązań umownych. Jeżeli posiadacz danych nie uczyni tego bez zbędnej zwłoki, użytkownik ma możliwość skorzystania ze środków ochrony prawnej przewidzianych w umowie dla przypadków istotnego naruszenia zobowiązania wynikającego z umowy.

Jeżeli użytkownik uzna, że jego prawo dostępu na mocy art. 4 ust. 1 aktu w sprawie danych zostało naruszone, jest również uprawniony do wniesienia skargi do właściwego organu wyznaczonego zgodnie z art. 37 ust. 5 lit. b) aktu w sprawie danych. Użytkownik powinien jednak mieć świadomość, że dokładne zadania i uprawnienia właściwych organów wyznaczonych zgodnie z art. 37 mogą się różnić w poszczególnych państwach członkowskich.

Użytkownik ma zawsze prawo do skorzystania ze skutecznego środka ochrony prawnej przed właściwym sądem lub do skierowania sporu do dowolnego organu oferującego alternatywne metody rozwiązywania sporów.
Użytkownik musi zatem starannie ocenić, jaki jest najbardziej odpowiedni sposób zobowiązania posiadacza danych do wypełnienia jego obowiązków prawnych lub zobowiązań umownych.

4.4. **Jednostronne zmiany dokonywane przez posiadacza danych**

4.4.1. Posiadacz danych może jednostronnie zmienić specyfikacje charakterystyki danych lub ustalenia dotyczące dostępu określone w **dodatku 1**, jeżeli jest to obiektywnie uzasadnione zwykłym prowadzeniem działalności gospodarczej przez posiadacza danych, na przykład modyfikacją techniczną wynikającą z bezpośredniego zagrożenia bezpieczeństwa w odniesieniu do linii produktów lub usług powiązanych lub zmianą infrastruktury posiadacza danych. Każda zmiana musi spełniać wymogi klauzul 4.2.1 i 4.2.2.

Posiadacz danych musi zawiadomić użytkownika o zmianie co najmniej (*wskazać rozsądny okres*) przed wejściem zmiany w życie.

Krótszy termin zawiadomienia może być wystarczający:

a) jeżeli zmiana nie ma negatywnego wpływu na dostęp do danych i ich wykorzystywanie przez użytkownika lub

b) jeżeli takie zawiadomienie byłoby niemożliwe lub nierozsądne w danych okolicznościach, na przykład gdy natychmiastowe zmiany są wymagane ze względu na wykrycie bezpośredniego zagrożenia bezpieczeństwa.

5. **(jeżeli dane udostępniane przez posiadacza danych na wniosek użytkownika muszą być chronione jako tajemnice przedsiębiorstwa) Ochrona tajemnic przedsiębiorstwa**

1. **Dzielenie się tajemnicami przedsiębiorstwa** – Posiadacze danych co do zasady nie mogą odrzucić wniosku o dostęp do danych wystosowanego na podstawie aktu w sprawie danych wyłącznie ze względu na to, że niektóre dane uznaje się za tajemnicę przedsiębiorstwa, ponieważ przeczyłoby to zamierzonym celom aktu w sprawie danych.

Zob. klauzule 5.1.

Tajemnice przedsiębiorstwa – Jeżeli jednak posiadacz danych stwierdzi, że niektóre dane objęte umową są chronione jako tajemnice przedsiębiorstwa w rozumieniu dyrektywy (UE) 2016/943 ([4]) (zwanej dalej „dyrektywą w sprawie tajemnic przedsiębiorstwa"), przysługują mu określone prawa, w szczególności prawo do zachowania poufności informacji stanowiących tajemnicę przedsiębiorstwa.

Zgodnie z art. 2 pkt 1 dyrektywy w sprawie tajemnic przedsiębiorstwa termin „tajemnica przedsiębiorstwa" oznacza informacje, które spełniają trzy wymogi: a) są poufne w tym sensie, że jako całość lub w szczególnym zestawie i zbiorze ich elementów nie są ogólnie znane lub łatwo dostępne dla osób z kręgów, które zwykle zajmują się tym rodzajem informacji, b) mają wartość handlową dlatego, że są objęte tajemnicą oraz c) poddane zostały przez osobę, która zgodnie z prawem sprawuje nad nimi kontrolę, rozsądnym, w danych okolicznościach, działaniom dla utrzymania ich w tajemnicy.

„Posiadacz tajemnicy przedsiębiorstwa" oznacza każdą osobę fizyczną lub prawną, która w sposób zgodny z prawem sprawuje kontrolę nad taką tajemnicą przedsiębiorstwa.

([4]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.U. L 157 z 15.6.2016, s. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Dane można zidentyfikować jako tajemnice przedsiębiorstwa tylko wtedy, gdy są one chronione jako takie przez posiadacza danych lub posiadacza tajemnicy przedsiębiorstwa w przypadku złożenia wniosku o dostęp do danych zgodnie z art. 4 aktu w sprawie danych.

Zob. klauzula 5.1.1.

2. **Początkowa identyfikacja tajemnic przedsiębiorstwa** – Prawa posiadaczy danych w odniesieniu do tajemnic przedsiębiorstwa mają – początkowo – zastosowanie wyłącznie wtedy, gdy i wyłącznie w takim zakresie, w jakim dane chronione jako tajemnice przedsiębiorstwa zostały zidentyfikowane w umowie.

Zob. klauzula 5.1.2.

3. **W trakcie obowiązywania umowy** – Prawa posiadaczy danych w odniesieniu do tajemnic przedsiębiorstwa mogą jednak mieć również zastosowanie w trakcie obowiązywania umowy w odniesieniu do nowych danych, które mają zostać udostępnione.

Zob. klauzula 5.1.3.

4. **Prawa do audytu** – W celu zachowania poufności danych chronionych jako tajemnice przedsiębiorstwa, nie ingerując wzajemnie w swoje działania, strony mogą rozważyć uwzględnienie pewnych praw do audytu realizowanych przez zaangażowanie niezależnych osób trzecich, w tym mechanizmów na wypadek sporów dotyczących wyników zawartych w sprawozdaniu z audytu. Strony mogą stosować środki alternatywne wobec audytu.

Zob. klauzula 5.2.3.

5. **Prawa posiadacza tajemnicy przedsiębiorstwa (1/4)** – Posiadacz danych (lub posiadacz tajemnicy przedsiębiorstwa będący osobą trzecią) może uzgodnić z użytkownikiem wymogi dotyczące zachowania poufności tajemnic przedsiębiorstwa jako warunek udostępnienia tych zidentyfikowanych tajemnic przedsiębiorstwa, takie jak wprowadzenie określonych proporcjonalnych środków technicznych i organizacyjnych.

Zob. klauzule 5.2. i 5.3.

6. **Prawa posiadacza tajemnicy przedsiębiorstwa (2/4)** – Jeżeli początkowe środki okażą się niewystarczające, posiadacz tajemnicy przedsiębiorstwa może, w zależności od przypadku, w odniesieniu do konkretnych i zidentyfikowanych danych chronionych jako tajemnice przedsiębiorstwa, jednostronnie zwiększyć poziom stosowanych środków albo zwrócić się o uzgodnienie z użytkownikiem dodatkowych środków. W przypadku braku porozumienia w sprawie niezbędnych środków posiadacz danych może zawiesić dzielenie się określonymi danymi chronionymi jako tajemnice przedsiębiorstwa na warunkach określonych w akcie w sprawie danych.

Zob. klauzula 5.4.1.

7. **Prawa posiadacza tajemnicy przedsiębiorstwa (3/4)** – Posiadacz tajemnicy przedsiębiorstwa może również, w zależności od przypadku, odmówić udostępnienia konkretnych, zidentyfikowanych tajemnic przedsiębiorstwa, jednak wyłącznie w wyjątkowych okolicznościach i na warunkach określonych w akcie w sprawie danych.

Zob. klauzula 5.4.2.

8. **Prawa posiadacza tajemnicy przedsiębiorstwa (4/4)** – Posiadacz tajemnicy przedsiębiorstwa może wstrzymać lub zawiesić dzielenie się danymi, jeżeli użytkownik narusza swoje obowiązki związane z ochroną tajemnic przedsiębiorstwa.

Zob. klauzula 5.4.3.

9. **Zatrzymywanie danych zawierających zidentyfikowane tajemnice przedsiębiorstwa** – Jeżeli posiadacz danych wstrzymuje lub zawiesza dzielenie się danymi zgodnie z klauzulami 5.4.1, 5.4.2 lub 5.4.3, posiadacz danych pozostaje zobowiązany do zapewnienia łatwego dostępu do powiązanych danych zawierających zidentyfikowane tajemnice przedsiębiorstwa przez ich zatrzymanie do czasu, gdy możliwe będzie ich udostępnienie w zakresie objętym umową.

Zob. klauzula 5.6.

10. **Posiadacz zidentyfikowanej tajemnicy przedsiębiorstwa będący osobą trzecią** – Jeżeli posiadacz tajemnicy przedsiębiorstwa jest osobą trzecią, posiadacz danych musi dopilnować, aby klauzula 5 chroniła również jego tajemnice przedsiębiorstwa, oraz uzyskać wszystkie odpowiednie upoważnienia od wspomnianego posiadacza tajemnicy przedsiębiorstwa będącego osobą trzecią.

Zob. klauzula 5.1.2.

5.1. **Stosowanie ustaleń dotyczących tajemnic przedsiębiorstwa**

5.1.1. Środki ochrony uzgodnione w klauzulach 5.2 i 5.3 niniejszej umowy, a także powiązane prawa uzgodnione w klauzuli 5.4 mają zastosowanie wyłącznie do danych lub metadanych zawartych w danych, które mają być udostępniane użytkownikowi przez posiadacza danych i które są chronione jako tajemnice przedsiębiorstwa (zgodnie z definicją zawartą w dyrektywie w sprawie tajemnic przedsiębiorstwa), będących w posiadaniu posiadacza danych lub innego posiadacza tajemnicy przedsiębiorstwa (zgodnie z definicją zawartą w tej dyrektywie).

5.1.2. Dane identyfikujące dane chronione jako tajemnice przedsiębiorstwa oraz tożsamość posiadaczy tajemnic przedsiębiorstwa określono w dodatku 4.

Posiadacz danych oświadcza użytkownikowi, że uzyskał wszystkie odpowiednie prawa od posiadacza tajemnic przedsiębiorstwa będącego osobą trzecią do zawarcia niniejszej umowy w odniesieniu do danych chronionych jako tajemnice przedsiębiorstwa.

Zgodnie z art. 4 ust. 6 aktu w sprawie danych „[p]osiadacz danych lub, jeżeli nie jest to ta sama osoba, posiadacz tajemnicy przedsiębiorstwa identyfikują dane chronione, w tym stosowne metadane, jako tajemnice przedsiębiorstwa".

W związku z tym posiadacz danych powinien zidentyfikować dane chronione jako tajemnice przedsiębiorstwa w **dodatku 4**. Posiadacz danych nie powinien być jednak zobowiązany do opisania samej tajemnicy przedsiębiorstwa. Wystarczy, że zidentyfikuje dane, które muszą być chronione w celu zapewnienia poufności tajemnicy przedsiębiorstwa, jeżeli analiza takich danych mogłaby skutkować ujawnieniem tajemnicy przedsiębiorstwa.

5.1.3. Jeżeli w trakcie obowiązywania niniejszej umowy użytkownikowi udostępnione zostaną nowe dane chronione jako tajemnice przedsiębiorstwa zgodnie z klauzulą 5.1.1, na wniosek posiadacza danych dodatek 4 zostanie odpowiednio zmieniony.

Do czasu zmiany i uzgodnienia przez strony treści **dodatku 4** posiadacz danych może wstrzymać lub tymczasowo zawiesić dzielenie się danymi chronionymi jako tajemnice przedsiębiorstwa. W takim przypadku posiadacz danych należycie uzasadnia decyzję i bez zbędnej zwłoki przekazuje ją na piśmie użytkownikowi. Posiadacz danych zawiadamia również właściwy organ wyznaczony na podstawie art. 37 rozporządzenia (UE) 2023/2854, że wstrzymał lub zawiesił dzielenie się danymi, oraz wskazuje, których środków nie uzgodniono lub nie wdrożono.

5.1.4. Zobowiązania określone w klauzulach 5.2 i 5.3 pozostają w mocy po rozwiązaniu umowy w jakikolwiek sposób, chyba że strony postanowią inaczej.

5.2. **Środki ochrony stosowane przez użytkownika**

5.2.1. Użytkownik jest zobowiązany stosować środki ochrony określone w **dodatku 4** (zwane dalej „środkami ochrony leżącymi w gestii użytkownika").

Strony powinny w odrębnym dodatku zawrzeć wszystkie szczegółowe informacje dotyczące tych środków, w tym sytuacji, gdy użytkownik dzieli się danymi z osobami trzecimi. Środki te mogą być zarówno techniczne (np. szyfrowanie, zapory sieciowe, przechowywanie danych w odrębnych lokalizacjach itp.), jak i organizacyjne (np. zarządzanie wewnętrzne, odpowiednie zarządzanie tożsamością i kontrole dostępu, zaangażowanie zaufanej osoby trzeciej, umowy o zachowanie poufności).

Ponieważ środki muszą być proporcjonalne, ich treść będzie się różnić w zależności od charakteru danej tajemnicy przedsiębiorstwa. Środki te będą również zależały od tego, czy (i) udziela się dostępu do danych w miejscu ich przechowywania lub czy będzie to (ii) pełne przekazanie danych użytkownikowi. W pierwszym przypadku posiadacz danych zachowuje wyższy stopień kontroli i może samodzielnie stosować część środków ochrony, podczas gdy użytkownik może mieć bardziej ograniczony zakres korzystania z danych. W każdym przypadku obie strony powinny koncentrować się na osiągnięciu zamierzonych skutków aktu w sprawie danych. Z tego względu konieczne jest wyważenie poszczególnych interesów, bez podważania tych zamierzonych skutków.

5.2.2. Jeżeli użytkownik jest uprawniony do udostępnienia danych osobie trzeciej, może udostępnić dane chronione jako tajemnice przedsiębiorstwa, jeżeli:

a) (i) bez zbędnej zwłoki poinformuje posiadacza danych o fakcie, że dane chronione jako tajemnice przedsiębiorstwa zostaną udostępnione osobie trzeciej, (ii) wskaże dane, których to dotyczy, oraz (iii) przekaże posiadaczowi danych informacje o tożsamości tej osoby trzeciej i jej miejscu prowadzenia działalności oraz dane kontaktowe tej osoby trzeciej;

b) osoba trzecia stosuje środki ochrony określone w dodatku 4.

5.2.3. [WARIANT] [W celu weryfikacji, czy i w jakim zakresie użytkownik wdrożył i utrzymuje środki ochrony leżące w gestii użytkownika, użytkownik zgadza się (i) albo co roku uzyskiwać na własny koszt sprawozdanie z audytu oceny zgodności w zakresie bezpieczeństwa od niezależnej osoby trzeciej wybranej przez użytkownika, albo (ii) na koszt posiadacza danych, co roku umożliwiać przeprowadzenie audytu oceny zgodności w zakresie bezpieczeństwa przez niezależną osobę trzecią wybraną przez posiadacza danych, pod warunkiem że taka niezależna osoba trzecia podpisała umowę o zachowanie poufności przedstawioną przez użytkownika. Takie sprawozdanie z audytu bezpieczeństwa musi potwierdzać przestrzeganie przez użytkownika klauzul 5 oraz dodatku 4, w brzmieniu obowiązującym w danej chwili. Wyniki sprawozdań z audytu są przekazywane obu stronom bez zbędnej zwłoki.

Użytkownik może dokonać wyboru pomiędzy wariantem (i) a wariantem (ii). Jeżeli strona uzna sprawozdanie z audytu bezpieczeństwa uzyskane na koszt drugiej strony za nieprawidłowe, zachowuje prawo do uzyskania sprawozdania z audytu bezpieczeństwa od innej niezależnej osoby trzeciej na własny koszt. W przypadku skorzystania z tego prawa obaj niezależni audytorzy będący osobami trzecimi, wraz ze stronami, omawiają wszelkie różnice między tymi dwoma sprawozdaniami i dążą do rozwiązania wszelkich nierozstrzygniętych kwestii, działając w dobrej wierze.]

Klauzula ta jest oznaczona jako wariant, ponieważ strony mogą uzgodnić inne środki służące weryfikacji, czy użytkownik wywiązuje się ze swoich zobowiązań w zakresie wdrażania i utrzymywania środków ochrony leżących w gestii użytkownika.

5.3. **Środki ochrony stosowane przez posiadacza tajemnicy przedsiębiorstwa**

5.3.1. Posiadacz danych może stosować środki uzgodnione w **dodatku 4** w celu zachowania poufności danych chronionych jako tajemnice przedsiębiorstwa (zwane dalej „środkami ochrony stosowanymi przez posiadacza danych").

5.3.2. Posiadacz danych może jednostronnie wdrożyć odpowiednie techniczne i organizacyjne rozwiązania ochronne, takie jak aktualizacja oprogramowania, jeżeli nie mają one negatywnego wpływu na użytkownika w ramach niniejszej umowy.

5.3.3. Użytkownik zobowiązuje się nie zmieniać ani nie usuwać środków ochrony stosowanych przez posiadacza danych ani środków stosowanych zgodnie z klauzulą 5.3.2, chyba że strony postanowią inaczej.

5.4. **Obowiązek dzielenia się danymi i prawo do odmowy, wstrzymania lub rozwiązania umowy**

5.4.1. W przypadku gdy środki ochrony leżące w gestii zidentyfikowanego użytkownika i środki ochrony stosowane przez posiadacza danych nie są zasadniczo wystarczające do zapewnienia właściwej ochrony określonego elementu danych chronionych jako tajemnica przedsiębiorstwa, posiadacz danych może zwrócić się o uzgodnienie dodatkowych środków ochrony przez skierowanie do użytkownika zawiadomienia zawierającego szczegółowy opis niewystarczalności tych środków. Jeżeli po upływie rozsądnego okresu nie zostanie osiągnięte porozumienie w sprawie niezbędnych dodatkowych środków i jeżeli potrzeba wprowadzenia takich środków zostanie należycie uzasadniona, np. w sprawozdaniu z audytu bezpieczeństwa, posiadacz danych może wstrzymać lub zawiesić dzielenie się konkretnymi danymi, których to dotyczy. W takim przypadku posiadacz danych musi zawiadomić użytkownika. Zawiadomienie to musi być należycie uzasadnione, wskazywać, które środki nie zostały uzgodnione oraz – w stosownych przypadkach – których tajemnic przedsiębiorstwa sprawa dotyczy, a także musi być przekazane na piśmie bez zbędnej zwłoki. Posiadacz danych jest obowiązany nadal dzielić się wszystkimi innymi danymi chronionymi jako tajemnice przedsiębiorstwa, z wyjątkiem tych konkretnych danych.

5.4.2. Jeżeli w wyjątkowych okolicznościach istnieje duże prawdopodobieństwo, że posiadacz danych poniesie poważną szkodę ekonomiczną w wyniku ujawnienia użytkownikowi określonych danych chronionych jako tajemnica przedsiębiorstwa pomimo wdrożenia środków ochrony leżących w gestii użytkownika i środków ochrony stosowanych przez posiadacza danych, posiadacz danych może odmówić dzielenia się tymi konkretnymi danymi lub zawiesić dzielenie się nimi.

Posiadacz danych musi bez zbędnej zwłoki przekazać użytkownikowi oraz właściwemu organowi wyznaczonemu zgodnie z art. 37 aktu w sprawie danych należycie uzasadnione zawiadomienie na piśmie.

Posiadacz danych jest jednak obowiązany nadal dzielić się wszystkimi innymi danymi chronionymi jako tajemnice przedsiębiorstwa, z wyjątkiem tych konkretnych danych.

Odmowa lub zaprzestanie dzielenia się danymi na podstawie art. 4 rozporządzenia (UE) 2023/2854 są ograniczone do wyjątkowych okoliczności. W związku z tym zawiadomienie musi być należycie uzasadnione. Aspekty, które należy uwzględnić, mogą obejmować na przykład brak możliwości wyegzekwowania ochrony tajemnic przedsiębiorstwa w państwach niebędących członkami UE, charakter i poziom poufności danej tajemnicy przedsiębiorstwa lub niepowtarzalność i nowatorski charakter danego produktu skomunikowanego.

5.4.3. Jeżeli użytkownik nie wdroży i nie będzie utrzymywał środków ochrony leżących w gestii użytkownika, a posiadacz danych należycie wykaże to uchybienie, na przykład w sprawozdaniu z audytu bezpieczeństwa, posiadacz danych jest uprawniony do wstrzymania lub zawieszenia dzielenia się konkretnymi zidentyfikowanymi tajemnicami przedsiębiorstwa do czasu, aż użytkownik zaradzi incydentowi.

W takim przypadku posiadacz danych musi bez zbędnej zwłoki przekazać użytkownikowi oraz właściwemu organowi wyznaczonemu zgodnie z art. 37 aktu w sprawie danych należycie uzasadnione zawiadomienie na piśmie.

5.4.4. Klauzula 5.4.1 nie uprawnia posiadacza danych do rozwiązania niniejszej umowy.

Klauzule 5.4.2 lub 5.4.3 uprawniają posiadacza danych do wypowiedzenia niniejszej umowy wyłącznie w odniesieniu do konkretnych zidentyfikowanych tajemnic przedsiębiorstwa oraz tylko wówczas, gdy:

a) wszystkie warunki określone w klauzulach 5.4.2 lub 5.4.3 zostały spełnione;

b) po upływie rozsądnego okresu strony nie osiągnęły porozumienia, pomimo podjęcia próby polubownego rozwiązania sporu, w tym po interwencji właściwego organu wyznaczonego na podstawie art. 37 aktu w sprawie danych, oraz

c) użytkownik nie uzyskał od właściwego sądu prawomocnego orzeczenia zobowiązującego posiadacza danych do udostępnienia danych, ani nie toczy się żadne postępowanie sądowe w sprawie wydania takiego orzeczenia.

5.5. **Zaprzestanie produkcji i zniszczenie towarów naruszających prawo**

Bez uszczerbku dla innych środków ochrony prawnej przysługujących posiadaczowi danych zgodnie z niniejszą umową lub prawem właściwym dla tej umowy, jeżeli użytkownik zmienia lub usuwa techniczne środki ochrony stosowane przez posiadacza danych lub nie utrzymuje środków technicznych i organizacyjnych zastosowanych przez niego w porozumieniu z posiadaczem danych zgodnie z klauzulami 5.2 i 5.3, posiadacz danych może zwrócić się do użytkownika o:

a) skasowanie danych udostępnionych przez posiadacza danych lub wszelkich ich kopii lub

b) zaprzestanie produkcji, oferowania, wprowadzania do obrotu lub wykorzystywania towarów, danych wywnioskowanych lub usług wytworzonych na podstawie wiedzy pozyskanej dzięki takim zidentyfikowanym tajemnicom przedsiębiorstwa lub przywozu, wywozu lub magazynowania do tych celów towarów naruszających prawo oraz zniszczenie wszelkich towarów naruszających prawo, w przypadku gdy istnieje poważne ryzyko, że niezgodne z prawem wykorzystywanie tych danych spowoduje znaczną szkodę dla posiadacza danych lub posiadacza tajemnicy przedsiębiorstwa, lub gdy taki środek nie byłby nieproporcjonalny w świetle interesów posiadacza danych lub posiadacza tajemnicy przedsiębiorstwa, lub

c) zrekompensowanie szkody stronie, która ją poniosła w wyniku niewłaściwego wykorzystania lub ujawnienia takich danych udostępnionych lub wykorzystanych niezgodnie z prawem.

5.6. **Zatrzymywanie danych chronionych jako zidentyfikowane tajemnice przedsiębiorstwa**

5.6.1. W przypadku gdy posiadacz danych korzysta z prawa do odmowy, wstrzymania lub zawieszenia dzielenia się danymi z użytkownikiem zgodnie z klauzulami 5.4.1, 5.4.2 oraz 5.4.3, musi zapewnić zatrzymywanie danych, tak aby dane te zostały udostępnione użytkownikowi:

a) po uzgodnieniu i wdrożeniu odpowiednich środków ochrony lub

b) po wydaniu wiążącej decyzji przez właściwy organ lub sąd zobowiązującej posiadacza danych do przekazania danych użytkownikowi.

Ten obowiązek zatrzymywania danych wygasa, gdy właściwy organ lub sąd w wiążącej decyzji zezwoli na usunięcie takich zatrzymywanych danych lub gdy umowa ulegnie rozwiązaniu.

5.6.2. Posiadacz danych poniesie niezbędne koszty zatrzymywania danych na podstawie klauzuli 5.6.1. Użytkownik pokryje jednak takie koszty w zakresie, w jakim wstrzymanie lub zawieszenie dzielenia się danymi następuje zgodnie z klauzulą 5.4.3.

6. **(jeżeli dane są udostępniane przez posiadacza danych na wniosek użytkownika) Wykorzystywanie danych przez użytkownika**

6.1. **Dopuszczalne wykorzystywanie danych i dzielenie się danymi**

6.1.1. Użytkownik może wykorzystywać dane udostępnione na jego wniosek przez posiadacza danych w dowolnym zgodnym z prawem celu oraz – w zakresie, w jakim dane zostały przekazane użytkownikowi lub mogą zostać przez niego pobrane – swobodnie dzielić się danymi, z zastrzeżeniem ograniczeń określonych w klauzuli 6.2.

6.2. **Ograniczenia dotyczące wykorzystywania danych i dzielenia się danymi**

6.2.1. Użytkownik zobowiązuje się:

a) nie wykorzystywać danych do opracowania produktu skomunikowanego konkurującego z produktem objętym niniejszą umową ani nie dzielić się w tym celu danymi z osobą trzecią;

b) nie wykorzystywać takich danych do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji producenta lub, w stosownym przypadku, posiadacza danych;

c) nie stosować środków przymusu ani nie nadużywać luk w infrastrukturze technicznej posiadacza danych, która ma chronić dane, w celu uzyskania dostępu do danych;

d) nie dzielić się danymi z osobą trzecią uznaną za strażnika dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925.

6.2.2. [WARIANT] [Ponadto, zgodnie z art. 4 ust. 2 aktu w sprawie danych, użytkownik oraz posiadacz danych uzgadniają następujące ograniczenia lub zakazy w odniesieniu do następującego przetwarzania (*wskazać odnośne przetwarzanie: dostęp do danych, ich wykorzystywanie lub dalsze dzielenie się danymi*), którego skutkiem byłoby naruszenie wymogów bezpieczeństwa dotyczących produktu określonych w prawie Unii (*wskazać odnośny prawny wymóg bezpieczeństwa*), prowadzące do poważnego zagrożenia dla zdrowia, bezpieczeństwa lub ochrony osób fizycznych.

Użytkownik zobowiązuje się nie (wskazać odpowiednie ograniczenia lub zakazy związane z wyżej wymienionym przetwarzaniem).]

7. **Dzielenie się danymi z odbiorcą danych na wniosek użytkownika**

7.1. **Udostępnianie danych odbiorcy danych**

7.1.1. Posiadacz danych jest obowiązany udostępnić odbiorcy danych, na wniosek przedstawiony przez użytkownika lub osobę działającą w jego imieniu, nieodpłatnie dla użytkownika, dane wraz z odpowiednimi metadanymi niezbędnymi do interpretacji i wykorzystania tych danych. Wniosek można złożyć na formularzu określonym w **dodatku 3**, wysyłając go na adres (*opisać procedurę dotyczącą zwykłego wniosku złożonego drogą elektroniczną, jeżeli jest to technicznie możliwe*). Do celów weryfikacji, czy wniosek został złożony przez użytkownika, od posiadacza danych nie wymaga się dostarczenia żadnych informacji poza tymi, które są niezbędne.

7.1.2. Jeżeli użytkownik nie jest osobą, której dane dotyczą, posiadacz danych udostępnia osobie trzeciej dane będące danymi osobowymi na wniosek użytkownika wyłącznie wówczas, gdy istnieje ważna podstawa prawna udostępnienia danych osobowych zgodnie z art. 6 rozporządzenia (UE) 2016/679 (RODO) oraz – w stosownych przypadkach – gdy spełnione są warunki określone w art. 9 tego rozporządzenia i art. 5 ust. 3 dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej).

W związku z tym, jeżeli użytkownik nie jest osobą, której dane dotyczą, w każdym wniosku składanym na podstawie poprzedniej klauzuli musi wskazać posiadaczowi danych podstawę prawną przetwarzania zgodnie z art. 6 rozporządzenia (UE) 2016/679 (oraz, w stosownych przypadkach, mające zastosowanie odstępstwo na podstawie art. 9 tego rozporządzenia i art. 5 ust. 3 dyrektywy 2002/58/WE), na której opiera się wniosek o udostępnienie danych osobowych.

7.1.3. Posiadacz danych jest obowiązany udostępnić dane odbiorcy danych, przy czym dane te muszą cechować się co najmniej taką samą jakością jak w chwili, gdy stały się dostępne dla posiadacza danych, i w każdym wypadku muszą być udostępnione w całościowym, ustrukturyzowanym, powszechnie używanym i nadającym się do odczytu maszynowego formacie, w sposób łatwy i bezpieczny.

7.1.4. Jeżeli użytkownik złoży taki wniosek, posiadacz danych uzgodni z odbiorcą danych warunki udostępnienia danych zgodnie z rozdziałami III i IV aktu w sprawie danych.

7.1.5. Użytkownik przyjmuje do wiadomości, że wniosek złożony na podstawie klauzuli 7.1.1 nie może przynieść korzyści osobie trzeciej uznanej za strażnika dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925 [WARIANT] [i nie może zostać złożony w kontekście testowania nowych produktów skomunikowanych, substancji lub procesów, które nie zostały jeszcze wprowadzone do obrotu].

7.1.6. Użytkownik przyjmuje do wiadomości, że osoba trzecia przetwarza dane udostępnione jej zgodnie z klauzulą 7.1.1 wyłącznie do celów i na warunkach uzgodnionych z użytkownikiem. Posiadacz danych nie ponosi wobec użytkownika odpowiedzialności za brak takiego porozumienia pomiędzy użytkownikiem a osobą trzecią, chyba że posiadacz danych wiedział lub powinien był wiedzieć o braku tego porozumienia.

8. **[WARIANT w przypadku gdy użytkownik jest podmiotem gospodarczym] Ograniczenia praw użytkownika**

Użytkownik zgadza się na (*określić cel, charakter i czas trwania ograniczenia prawa użytkownika do wykorzystywania danych lub dzielenia się danymi oraz określić część danych, której dotyczą takie ograniczenia*).

Zgodnie z art. 7 ust. 2 aktu w sprawie danych „[p]ostanowienie umowne, które ze szkodą dla użytkownika wyklucza stosowanie praw użytkownika przewidzianych w [rozdziale II], stanowi odstępstwo od nich lub zmienia ich skutek, nie jest dla użytkownika wiążące".

Przepis ten należy odczytywać w świetle motywu 25, który stanowi, że „nie uniemożliwia [on] użytkownikom, w przypadku stosunków między przedsiębiorcami, udostępniania danych osobom trzecim lub posiadaczom danych na podstawie zgodnych z prawem postanowień umownych, w tym poprzez uzgodnienie ograniczenia lub zawężenia dalszego dzielenia się takimi danymi; nie uniemożliwia im także otrzymania proporcjonalnej rekompensaty, np. w zamian za zrzeczenie się prawa do wykorzystywania takich danych lub dzielenia się nimi".

W związku z tym takie ograniczenia będą ważne wyłącznie wtedy, gdy nie powodują szkody dla użytkownika, co oznacza, że powinny nie naruszać uzasadnionych interesów użytkownika.

Ponadto klauzula ta nie powinna być stosowana w sposób prowadzący do całkowitego pozbawienia użytkownika jego praw wynikających z art. 4 i 5 aktu w sprawie danych, na przykład przez całkowite zrzeczenie się przez użytkownika prawa dostępu do danych. Użytkownik może zgodzić się na ograniczenia swoich praw wyłącznie wówczas, gdy mają one ograniczony zakres przedmiotowy i czasowy oraz nie działają na jego niekorzyść. Mogą to być na przykład szczególne ograniczenia dotyczące wykorzystywania danych, do których uzyskano dostęp, lub uzgodnienie, że dane nie będą dalej udostępniane osobie trzeciej, jak wskazano w motywie 25, lub że odbiorca danych nie będzie dalej dzielił się danymi z osobą trzecią.

Klauzula ta może być stosowana w sytuacjach, w których użytkownik ma interes w ustanowieniu takich ograniczeń, na przykład gdy posiadacz danych i użytkownik realizują wspólny projekt przemysłowy.

Może ona mieć również zastosowanie, jeżeli użytkownik otrzymuje rekompensatę. Samo otrzymanie rekompensaty nie byłoby jednak wystarczające, aby uznać, że ograniczenia nie działają na niekorzyść użytkownika. Rekompensata powinna być proporcjonalna do ograniczeń.

Użytkownik może, według własnego uznania, zaakceptować lub odrzucić ograniczenia na podstawie tej klauzuli.

9. **Rekompensata dla użytkownika**

9.1. **Rekompensata**

Posiadacz danych zobowiązuje się do wypłacenia użytkownikowi rekompensaty, jak określono szczegółowo w **dodatku 7** (*w stosownych przypadkach*), w tym z tytułu ograniczeń praw użytkownika zgodnie z klauzulą 8.

Strony mogą uzgodnić rekompensatę za wykorzystywanie danych i dzielenie się danymi przez posiadacza danych, jeżeli uznają to za sprawiedliwe i zasadne. Mogą na przykład rozważyć taką rekompensatę w sytuacji, gdy posiadacz danych wykorzystuje dane do opracowywania nowych produktów lub usług lub gdy posiadacz danych tworzy dane zagregowane lub wywnioskowane do celów komercyjnych. Natomiast w przypadku, gdy na przykład dane są wykorzystywane wyłącznie na potrzeby jakiejkolwiek umowy zawartej z użytkownikiem lub w celu zapewnienia funkcjonowania, bezpieczeństwa i ochrony produktu lub usługi powiązanej, umowa może nie przewidywać rekompensaty.

Strony powinny jednak mieć świadomość, że na przykład w przypadku gdy użytkownik ogranicza swoje prawa zgodnie z klauzulą 8, powinien on otrzymać rekompensatę, jak wyjaśniono w ramce objaśniającej w klauzuli 8, a rekompensata powinna być proporcjonalna do wagi ograniczenia.

Podobnie w celu zapewnienia sprawiedliwego traktowania użytkownika rekompensata może być potrzebna, jeżeli użytkownik zgadza się na to, by posiadacz danych mógł sprzedawać dane osobom trzecim zgodnie z klauzulą 3.2.1 lit. a) pkt (iii).

Jeżeli rekompensata jest należna, strony muszą uzgodnić jej charakter, który może mieć formę pieniężną lub niepieniężną.

9.2. **(dotyczy rekompensaty pieniężnej) Odsetki za opóźnienia w płatnościach**

W przypadku opóźnienia w zapłacie rekompensaty posiadacz danych powinien zapłacić użytkownikowi odsetki od zaległej rekompensaty za okres od dnia, w którym płatność stała się wymagalna, do dnia jej dokonania, zgodnie z prawem właściwym.

10. **Przeniesienie prawa do korzystania oraz wielu użytkowników**

Pierwotny użytkownik może na stałe przenieść własność produktu lub swoje prawo do korzystania z produktu na kolejnego użytkownika, na przykład w przypadku sprzedaży produktu (przeniesienie prawa do korzystania).

Pierwotny użytkownik może również przyznać prawa do korzystania z produktu lub do otrzymywania usług powiązanych dodatkowym użytkownikom, zachowując jednocześnie swoją rolę użytkownika (przypadek istnienia wielu użytkowników), na przykład gdy:

— przedsiębiorstwo podnajmuje swój samochód dostawczy innemu przedsiębiorstwu na niektóre okresy w ciągu roku;

— wypożyczalnia samochodów wynajmuje swoje samochody klientom.

Prawo posiadacza danych do wykorzystywania danych

W takich przypadkach posiadacz danych musi zawrzeć umowę z kolejnym użytkownikiem lub dodatkowym użytkownikiem, aby móc wykorzystywać dane wygenerowane w wyniku korzystania z produktu lub usług powiązanych przez tych użytkowników. W poniższych klauzulach zaproponowano możliwe rozwiązania dotyczące zawarcia takiej umowy, tak aby strony mogły wybrać rozwiązanie, które jest najbardziej dostosowane do specyfiki sytuacji.

W przypadku przeniesienia prawa do korzystania strony mogą na przykład uzgodnić, że pierwotny użytkownik powiadomi posiadacza danych o przeniesieniu, tożsamości oraz danych kontaktowych kolejnego użytkownika, tak aby posiadacz danych mógł skontaktować się z kolejnym użytkownikiem i zawrzeć z nim umowę.

W przypadku istnienia wielu użytkowników takie rozwiązanie może być zbyt uciążliwe dla posiadacza danych. Jeżeli pierwotny użytkownik jest w stanie działać w imieniu posiadacza danych, jedną z możliwości jest uzyskanie przez pierwotnego użytkownika zgody dodatkowych użytkowników na warunki dostępu do danych i ich wykorzystywania określone w niniejszej umowie.

W innych sytuacjach nadal może być wykonalne i pożądane, aby pierwotny użytkownik przekazał posiadaczowi danych dane kontaktowe dodatkowego użytkownika w taki sposób, aby posiadacz danych mógł zawrzeć umowę bezpośrednio z dodatkowym użytkownikiem.

Możliwa jest również sytuacja, w której posiadacz danych nie musi być powiadamiany przez pierwotnego użytkownika o kolejnym lub dodatkowym użytkowniku w celu zawarcia umowy, ponieważ okoliczności są takie, że posiadacz danych może zawrzeć umowę bez jakiegokolwiek działania ze strony pierwotnego użytkownika. Na przykład może się zdarzyć, że do korzystania z produktu lub usługi powiązanej wymagane jest utworzenie konta identyfikującego użytkownika. W takim przypadku posiadacz danych będzie w stanie zawrzeć umowę z kolejnym lub dodatkowym użytkownikiem w momencie, gdy utworzą oni własne konta. Może to jednak wymagać od pierwotnego użytkownika zapewnienia, aby kolejny użytkownik lub dodatkowy użytkownik nie korzystali z jego konta.

Prawa dostępu stron w przypadku przeniesienia prawa do korzystania oraz wielu użytkowników

W przypadku przeniesienia prawa do korzystania lub w przypadku istnienia wielu użytkowników umowa powinna zapewniać jasność co do tego, kto może uzyskać dostęp do danych i na jakich warunkach. Na przykład w przypadku gdy przedsiębiorstwo (pierwotny użytkownik) wynajmuje skomunikowane maszyny rolnicze indywidualnym rolnikom (dodatkowym użytkownikom) na doby lub tygodnie, dane generowane przez maszyny rolnicze mogą ujawniać szczególnie chronione informacje handlowe poszczególnych rolników. Producent (posiadacz danych) nie może po prostu udostępnić jakichkolwiek danych na podstawie klauzuli 4 niniejszej umowy pierwotnemu użytkownikowi (przedsiębiorstwu będącemu właścicielem maszyn) bez upewnienia się, że w ten sposób nie zostaną naruszone żadne informacje poufne ani prawa indywidualnych rolników (dodatkowych użytkowników).

Prawa dostępu dodatkowego lub kolejnego użytkownika mogą w szczególności zależeć od umownej kategoryzacji danych, na przykład:

— dane usuwalne przez użytkownika – produkty lub usługi powiązane często umożliwiają użytkownikowi usunięcie danych wygenerowanych podczas korzystania z tych produktów lub usług. W przypadku przeniesienia prawa do korzystania użytkownik powinien usunąć takie dane. W przeciwnym razie takie dane mogą być dostępne dla dodatkowego lub kolejnego użytkownika;

— dane zawsze usuwalne – dane, których posiadacz danych nie powinien udostępniać dodatkowemu użytkownikowi ani kolejnemu użytkownikowi;

— pozostałe dane – dane inne niż dane usuwalne przez użytkownika lub dane zawsze usuwalne; takie dane nie będą usuwalne i nie będą podlegać umowie o zachowanie poufności (tj. dane będą również dostępne dla nowych kolejnych użytkowników). Takie dane mogą obejmować dane, które muszą być dostępne dla dodatkowego lub kolejnego użytkownika z mocy prawa lub w praktyce (na przykład dane związane z aktualizacjami wprowadzanymi w pojeździe podłączonym do internetu).

Posiadacz danych powinien podzielić dane na te kategorie, w szczególności w informacjach, o których mowa w art. 3 ust. 2 i 3 aktu w sprawie danych, w niniejszej umowie (np. w dodatku 1) lub w dokumentacji dotyczącej produktu lub usługi powiązanej.

W klauzuli 10 skoncentrowano się na akcie w sprawie danych; nie ma ona wpływu na żadne dodatkowe przepisy, w tym przepisy sektorowe, które mogą regulować przeniesienie prawa do korzystania z produktu skomunikowanego lub usługi powiązanej (np. regenerację wyrobów medycznych).

10.1. **Przeniesienie prawa do korzystania**

W przypadku gdy użytkownik przenosi na mocy umowy (i) własność produktu lub (ii) przysługujące mu tymczasowe prawa do korzystania z produktu lub (iii) przysługujące mu prawa do otrzymywania usług powiązanych na kolejną osobę („kolejny użytkownik") i po dokonaniu przeniesienia traci status użytkownika, strony zobowiązują się do przestrzegania wymogów określonych w niniejszej klauzuli.

[WARIANT 1] [Pierwotny użytkownik musi zawiadomić posiadacza danych o przeniesieniu i przekazać mu niezbędne dane kontaktowe kolejnego użytkownika, tak aby posiadacz danych mógł z nim zawrzeć umowę dotyczącą wykorzystania danych przez posiadacza danych.]

[WARIANT 2] [Posiadacz danych podejmuje niezbędne kroki w celu zawarcia z kolejnym użytkownikiem umowy dotyczącej wykorzystania danych przez posiadacza danych. (*w stosownych przypadkach*) Pierwotny użytkownik musi zapewnić, aby kolejny użytkownik nie mógł korzystać z konta pierwotnego użytkownika.]

Przeniesienie nie będzie miało wpływu na prawa posiadacza danych do wykorzystywania danych z produktu lub danych z usług powiązanych wygenerowanych przed przeniesieniem, tj. prawa i obowiązki związane z danymi przekazanymi na podstawie umowy przed przeniesieniem pozostają w mocy po jego dokonaniu.

10.2. **Wielu użytkowników**

W przypadku gdy pierwotny użytkownik przyznaje prawo do korzystania z produktu lub usług powiązanych innej stronie („dodatkowy użytkownik"), zachowując jednocześnie swój status użytkownika, strony zobowiązują się do przestrzegania wymogów określonych w niniejszej klauzuli.

10.2.1. Zgoda dodatkowego użytkownika na wykorzystywanie danych i dzielenie się danymi przez posiadacza danych

[WARIANT 1] [W umowie między pierwotnym użytkownikiem a dodatkowym użytkownikiem pierwotny użytkownik zawiera, w imieniu posiadacza danych, klauzule odzwierciedlające merytorycznie treść niniejszej umowy między pierwotnym użytkownikiem a posiadaczem danych, a w szczególności klauzulę 3, dotyczącą wykorzystywania danych i dzielenia się danymi z produktu lub danymi z usług powiązanych przez posiadacza danych, na okres tymczasowego korzystania z produktu lub usługi powiązanej.]

[WARIANT 2] [Pierwotny użytkownik powiadamia posiadacza danych o istnieniu i okresie obowiązywania praw dodatkowego użytkownika do korzystania z produktu lub usługi powiązanej oraz przekazuje jego dane kontaktowe, tak aby posiadacz danych mógł zawrzeć z dodatkowym użytkownikiem umowę o wykorzystywanie tych danych i dzielenie się tymi danymi przez posiadacza danych.]

[WARIANT 3] [Posiadacz danych podejmuje niezbędne kroki w celu zawarcia umowy z dodatkowym użytkownikiem. (*w stosownych przypadkach*) Pierwotny użytkownik musi zapewnić, aby dodatkowy użytkownik nie mógł korzystać z konta pierwotnego użytkownika.]

10.2.2. Dostęp dodatkowego użytkownika do danych

[WARIANT] [Pierwotny użytkownik pełni funkcję pierwszego punktu kontaktowego dla dodatkowego użytkownika, jeżeli dodatkowy użytkownik złoży wniosek o dostęp do danych na podstawie art. 4 lub 5 aktu w sprawie danych. Posiadacz danych musi współpracować z pierwotnym użytkownikiem w celu rozpatrzenia wniosku, jak określono w **dodatku 10**.]

10.3. **Odpowiedzialność pierwotnego użytkownika**

W zakresie, w jakim niewypełnienie przez pierwotnego użytkownika jego zobowiązań wynikających z klauzul 10.1 i 10.2 doprowadzi do wykorzystywania danych oraz dzielenia się danymi z produktu lub danymi z usługi powiązanej przez posiadacza danych mimo braku umowy z kolejnym lub dodatkowym użytkownikiem, pierwotny użytkownik zabezpieczy posiadacza danych przed odpowiedzialnością z tytułu wszelkich roszczeń odszkodowawczych zgłaszanych wobec posiadacza danych przez kolejnego lub dodatkowego użytkownika z tytułu wykorzystywania danych po przekazaniu lub rozpoczęciu tymczasowego korzystania z produktu lub usług powiązanych.

11. **Data rozpoczęcia stosowania, okres obowiązywania i rozwiązanie umowy**

11.1. **Data rozpoczęcia stosowania i okres obowiązywania**

Ta umowa co do zasady nie funkcjonuje jako samodzielna umowa, lecz jest zawierana równolegle z umową przenoszącą własność produktu na użytkownika, umową przyznającą mu tymczasowe prawa do korzystania z produktu lub umową o świadczenie usługi powiązanej.

Umowa musi zatem zasadniczo pozostać w mocy tak długo, jak długo ta druga umowa umożliwia użytkownikowi korzystanie z produktu lub usługi powiązanej. Podobnie ani posiadacz danych, ani użytkownik nie powinni mieć możliwości rozwiązania niniejszej umowy, z wyjątkiem przypadku istotnego naruszenia zobowiązań przez drugą stronę, ponieważ w przeciwnym razie doprowadziłoby to do sytuacji, w której użytkownik korzysta z produktu lub usługi powiązanej bez żadnych ram umownych dotyczących praw i obowiązków wynikających z aktu w sprawie danych.

11.1.1. Niniejsza umowa [WARIANT 1] [wchodzi w życie ze skutkiem natychmiastowym] [WARIANT 2] [wchodzi w życie z dniem (*wskazać datę*)].

11.1.2. Niniejsza umowa zostaje zawarta [WARIANT 1] [na czas nieokreślony] [WARIANT 2] [na czas określony (*wskazać*)], z zastrzeżeniem wszelkich podstaw do jej wygaśnięcia lub rozwiązania przewidzianych w niniejszej umowie.

11.2. **Rozwiązanie umowy**

Niezależnie od okresu obowiązywania umowy uzgodnionego na mocy klauzuli 11.1 niniejsza umowa ulega rozwiązaniu:

a) z chwilą zniszczenia produktu lub trwałego zaprzestania świadczenia usługi powiązanej lub gdy produkt lub usługa powiązana w sposób nieodwracalny utracą zdolność generowania danych lub

b) z chwilą utraty przez użytkownika własności produktu lub z chwilą wygaśnięcia praw użytkownika do produktu wynikających z umowy najmu, dzierżawy, leasingu lub podobnej umowy, bądź wygaśnięcia praw użytkownika do usługi powiązanej lub

c) jeżeli obie strony tak postanowią.

Lit. b) i c) pozostają bez uszczerbku dla dalszego obowiązywania umowy między posiadaczem danych a każdym kolejnym lub dodatkowym użytkownikiem.

11.3. **Skutki wygaśnięcia i rozwiązania umowy**

11.3.1. Wygaśnięcie okresu obowiązywania umowy lub rozwiązanie niniejszej umowy zwalnia obie strony z zobowiązania do wykonania oraz do przyjęcia przyszłego świadczenia, lecz nie wpływa na prawa i zobowiązania, które powstały do chwili rozwiązania umowy.

Wygaśnięcie lub rozwiązanie umowy nie wpływa na postanowienia niniejszej umowy, które mają obowiązywać również po jej zakończeniu, w szczególności na klauzulę 13.1 – dotyczącą poufności, klauzulę 13.4 – dotyczącą prawa właściwego, oraz klauzulę 13.6 – dotyczącą rozstrzygania sporów.

11.3.2. Rozwiązanie lub wygaśnięcie umowy wywołuje następujące skutki:

a) posiadacz danych zaprzestaje pobierania wygenerowanych lub zarejestrowanych danych z dniem rozwiązania lub wygaśnięcia umowy;

b) posiadacz danych pozostaje uprawniony do wykorzystywania danych i dzielenia się danymi, które zostały wygenerowane lub zarejestrowane przed datą rozwiązania lub wygaśnięcia określoną w niniejszej umowie.

12. **Środki ochrony prawnej w przypadku naruszenia umowy**

Strony mogą uzgodnić nie tylko prawa i obowiązki dotyczące danych (z których wiele wynika już z aktu w sprawie danych), ale również kwestie z zakresu ogólnego prawa zobowiązań, takie jak prawa i środki ochrony prawnej przysługujące stronie umowy w przypadku niewykonania zobowiązania przez drugą stronę umowy.

W odniesieniu do takich kwestii z zakresu ogólnego prawa zobowiązań strony mogą chcieć oprzeć się na ustawowych przepisach dyspozytywnych lub na innych wzorach umów. Jeżeli chcą skorzystać z niniejszych modelowych postanowień umownych, powinny upewnić się, że są one zgodne z wszelkimi bezwzględnie obowiązującymi przepisami prawa krajowego, które mogą mieć zastosowanie do niniejszej umowy.

12.1. **Przypadki niewykonania zobowiązania**

12.1.1. Niewykonanie zobowiązania przez stronę jest istotnym naruszeniem zobowiązania wynikającego z niniejszej umowy, jeżeli:

a) niewykonanie zobowiązania w znacznym stopniu pozbawia drugą stronę tego, czego miała prawo oczekiwać na podstawie niniejszej umowy, chyba że strona, która nie wykonała zobowiązania, nie przewidziała i nie mogła w rozsądny sposób przewidzieć takiego rezultatu, lub

b) z okoliczności jasno wynika, że nie można polegać na przyszłym wykonaniu zobowiązań przez stronę, która nie wykonała zobowiązania.

12.1.2. Niewykonanie zobowiązania przez stronę jest usprawiedliwione, jeżeli wynika z przeszkody pozostającej poza jej kontrolą oraz jeżeli nie można było w rozsądny sposób oczekiwać, aby w chwili zawarcia niniejszej umowy strona ta uwzględniła tę przeszkodę bądź jej uniknęła lub przezwyciężyła ją lub jej skutki.

Jeżeli przeszkoda jest tylko tymczasowa, niewykonanie zobowiązania jest usprawiedliwione tylko w okresie, w którym istnieje przeszkoda. Jeżeli jednak opóźnienie stanowi istotne naruszenie zobowiązania, druga strona może je tak traktować.

Strona, która nie wykonała zobowiązania, ma obowiązek dopilnować, aby zawiadomienie o przeszkodzie oraz jej wpływie na możliwość wykonania zobowiązania dotarło do drugiej strony bez zbędnej zwłoki po tym, jak strona, która nie wykonała zobowiązania, dowiedziała się lub powinna była się dowiedzieć o tych okolicznościach. Druga strona jest uprawniona do odszkodowania za szkodę ekonomiczną wynikłą z nieotrzymania takiego zawiadomienia.

12.2. **Środki ochrony prawnej**

12.2.1. W przypadku niewykonania zobowiązania przez jedną ze stron drugiej stronie przysługują środki ochrony prawnej wymienione w poniższych klauzulach, bez uszczerbku dla wszelkich środków ochrony prawnej dostępnych na podstawie prawa właściwego.

12.2.2. Dopuszczalne jest łączenie środków ochrony prawnej, które wzajemnie się nie wykluczają.

12.2.3. Strona nie może skorzystać ze środka ochrony prawnej w zakresie, w jakim sama spowodowała niewykonanie zobowiązania przez drugą stronę, na przykład gdy uchybienie w jej własnej infrastrukturze danych uniemożliwiło drugiej stronie należyte wykonanie jej zobowiązań. Strona nie może również powoływać się na roszczenie odszkodowawcze z tytułu poniesionych szkód w zakresie, w jakim mogła ograniczyć powstałą szkodę przez podjęcie zasadnych kroków.

12.2.4. Strona poszkodowana może:

a) żądać, aby strona, która nie wykonała zobowiązania, bez zbędnej zwłoki wykonała swoje zobowiązania wynikające z niniejszej umowy, chyba że byłoby to niezgodne z prawem lub niemożliwe lub wykonanie zobowiązania powodowałoby dla strony, która nie wykonała zobowiązania, koszty niewspółmierne do korzyści, jakie uzyskałaby druga strona;

b) żądać, aby strona, która nie wykonała zobowiązania, skasowała dane, do których uzyskała dostęp lub które wykorzystywała z naruszeniem niniejszej umowy, oraz wszelkie ich kopie;

c) dochodzić odszkodowania za szkodę ekonomiczną poniesioną w wyniku niewykonania zobowiązania przez drugą stronę, jeżeli to niewykonanie nie jest usprawiedliwione na mocy klauzuli 12.1.2. Strona, która nie wykonała zobowiązania, ponosi odpowiedzialność wyłącznie za szkodę, którą przewidywała lub którą mogła w rozsądny sposób przewidzieć w chwili zawarcia niniejszej umowy jako skutek niewykonania zobowiązania, chyba że niewykonanie zobowiązania miało charakter umyślny lub stanowiło rażące zaniedbanie.

12.2.5. Posiadacz danych może również zawiesić dzielenie się danymi z użytkownikiem do czasu, aż użytkownik wywiąże się ze swoich zobowiązań lub zacznie przestrzegać nałożonych na niego ograniczeń – przekazując użytkownikowi należycie uzasadnione zawiadomienie bez zbędnej zwłoki:

a) jeżeli niewykonanie zobowiązania przez użytkownika jest istotnym naruszeniem zobowiązania;

b) (*w stosownych przypadkach*) pod warunkiem że spełnione są wszystkie pozostałe warunki określone w klauzuli 5.4.3 – w przypadkach opisanych w klauzuli 5.4.3.

12.2.6. Użytkownik może również:

a) zawiesić zgodę udzieloną posiadaczowi danych na podstawie klauzuli 3 lub swoją zgodę na ograniczenia praw użytkownika uzgodnione na mocy klauzuli 8 do czasu, aż posiadacz danych wywiąże się ze swoich zobowiązań, chyba że spowodowałoby to po stronie posiadacza danych uszczerbek rażąco niewspółmierny do niewykonania zobowiązania lub jego skutków;

b) cofnąć zgodę udzieloną posiadaczowi danych na podstawie klauzuli 3 lub swoją zgodę na ograniczenia praw użytkownika uzgodnione na mocy klauzuli 8 – przez przekazanie zawiadomienia posiadaczowi danych – jeżeli:

(i) niewykonanie zobowiązania przez posiadacza danych jest istotnym naruszeniem zobowiązania lub

(ii) w przypadku niewykonania, które nie stanowi istotnego naruszenia zobowiązania, użytkownik przekazał zawiadomienie wyznaczające rozsądny termin na usunięcie uchybienia, a termin ten upłynął bez wykonania zobowiązania przez posiadacza danych. Wskazany termin uznaje się za rozsądny, jeżeli posiadacz danych nie zgłosi wobec niego sprzeciwu bez zbędnej zwłoki.

12.2.7. [WARIANT] [W przypadku gdy strona nie wykona swoich zobowiązań wynikających z niniejszej umowy, jest ona w każdym przypadku zobowiązana do zapłaty kar umownych określonych szczegółowo w dodatku 8, które strony uznają za odszkodowanie w rozumieniu klauzuli 12.2.4 lit. c). Stronie, która nie wykonała zobowiązania, przysługuje prawo żądania obniżenia kary do rozsądnej wysokości, jeżeli strona ta wykaże, że kara jest rażąco wygórowana w stosunku do szkody wynikającej z niewykonania zobowiązania.]

Strony mogą określić kary za określone rodzaje niewykonania zobowiązania, ponieważ udowodnienie przez stronę poszkodowaną kwoty rzeczywistej szkody spowodowanej np. niedostarczeniem danych może być zbyt uciążliwe. Kary powinny być proporcjonalne.

13. **Postanowienie ogólne**

13.1. **Poufność**

13.1.1. Następujące informacje będą uważane za poufne:

a) informacje odnoszące się do tajemnic przedsiębiorstwa, sytuacji finansowej lub jakiegokolwiek innego aspektu działalności strony, chyba że dana strona sama podała te informacje do publicznej wiadomości;

b) informacje dotyczące użytkownika i wszelkich osób trzecich, chyba że informacje te zostały już podane przez nich do wiadomości publicznej.

13.1.2. Obie strony zgadzają się zastosować wszelkie uzasadnione środki w celu bezpiecznego przechowywania informacji poufnych i nie udostępniać takich informacji osobom trzecim, chyba że:

a) jedna ze stron jest prawnie zobowiązana do udostępnienia odpowiednich informacji;

b) jedna ze stron musi udostępnić odpowiednie informacje w celu wypełnienia swoich zobowiązań wynikających z niniejszej umowy lub

c) jedna ze stron uzyskała uprzednią zgodę drugiej strony lub strony, która przekazała informacje poufne lub której ujawnienie tych informacji dotyczy.

13.1.3. Te zobowiązania do zachowania poufności pozostają w mocy po rozwiązaniu niniejszej umowy przez okres (*wskazać okres*).

13.1.4. Te zobowiązania do zachowania poufności nie znoszą ani nie ograniczają bardziej rygorystycznych obowiązków wynikających z (i) rozporządzenia (UE) 2016/679 (RODO), (ii) przepisów wdrażających dyrektywę 2002/58/WE lub dyrektywę (UE) 2016/943 ani (iii) żadnego innego prawa Unii ani prawa państwa członkowskiego, ani (iv) (w stosownych przypadkach) klauzuli 6 niniejszej umowy.

13.2. **Środki komunikacji**

Wszelkie zawiadomienia lub inne komunikaty wymagane na mocy niniejszej umowy muszą mieć formę pisemną i mogą być doręczane osobiście, wysyłane pocztą przesyłką opłaconą z góry lub przekazywane drogą elektroniczną, w tym pocztą elektroniczną, pod warunkiem że nadawca zachowa dowód wysłania na adresy wskazane poniżej:

Strona	Osoba wyznaczona do kontaktów	E-mail	Telefon	Adres
Użytkownik	[Imię i nazwisko]/[Stanowisko]	[E-mail]	[Telefon]	[Adres]
Odbiorca danych	[Imię i nazwisko]/[Stanowisko]	[E-mail]	[Telefon]	[Adres]

Każde takie zawiadomienie lub każdy taki komunikat uznaje się za otrzymane:

a) w przypadku doręczenia osobistego – w dniu doręczenia,

b) w przypadku wysłania pocztą przesyłką opłaconą z góry – w trzecim dniu roboczym po dniu nadania,

c) w przypadku przekazania drogą elektroniczną – w dniu przekazania, pod warunkiem że nadawca nie otrzymał żadnego komunikatu o błędzie wskazującego na niedoręczenie.

13.3. **Całość umowy, zmiany i rozdzielność postanowień**

13.3.1. Niniejsza umowa (wraz z dodatkami do niej oraz wszelkimi innymi dokumentami, o których mowa w niniejszej umowie) stanowi całość umowy między stronami w odniesieniu do jej przedmiotu i zastępuje wszelkie wcześniejsze umowy, porozumienia i uzgodnienia stron – zarówno ustne, jak i pisemne – dotyczące przedmiotu niniejszej umowy.

13.3.2. Wszelkie zmiany niniejszej umowy są ważne wyłącznie wtedy, gdy zostaną uzgodnione na piśmie, w tym w jakiejkolwiek formie elektronicznej.

13.3.3. Jeżeli którekolwiek postanowienie niniejszej umowy zostanie uznane za nieważne, bezskuteczne, wzruszalne lub niewykonalne z jakiegokolwiek powodu i jeżeli postanowienie to można oddzielić od pozostałych postanowień umowy, te pozostałe postanowienia pozostaną ważne i wykonalne. Wszelkie powstałe w ten sposób luki lub niejasności w niniejszej umowie rozstrzyga się zgodnie z klauzulą 13.5.

13.4. **Prawo właściwe**

13.4.1. Niniejsza umowa podlega prawu (*określić państwo członkowskie*).

13.5. **Interpretacja**

13.5.1. Strony zawierają niniejszą umowę w kontekście praw i obowiązków stron wynikających z aktu w sprawie danych. Każde postanowienie niniejszej umowy należy interpretować w sposób zapewniający zgodność z aktem w sprawie danych oraz innymi przepisami prawa Unii lub przepisami krajowymi przyjętymi zgodnie z prawem Unii, a także z wszelkimi mającymi zastosowanie przepisami prawa krajowego, które są zgodne z prawem Unii i których nie można wyłączyć w drodze umowy.

13.5.2. Jeżeli jakiejkolwiek luki lub niejasności w niniejszej umowie nie można usunąć w sposób, o którym mowa w klauzuli 13.5.1, umowę tę należy interpretować w świetle zasad wykładni przewidzianych w prawie właściwym (zob. klauzula 13.4).

13.6. **Rozstrzyganie sporów**

13.6.1. Strony uzgadniają, że dołożą wszelkich starań w celu polubownego rozstrzygania sporów i że przed wniesieniem sprawy do sądu przekażą spór do (*wstawić nazwę i dane kontaktowe konkretnego organu rozstrzygania sporów; w odniesieniu do sporów mieszczących się w zakresie jego kompetencji określonych w art. 10 ust. 1 aktu w sprawie danych może to być każdy organ rozstrzygania sporów w państwie członkowskim, który spełnia warunki określone w art. 10 aktu w sprawie danych*).

13.6.2. Przekazanie sporu do organu rozstrzygania sporów zgodnie z klauzulą 13.6.1 nie narusza jednak prawa użytkownika do wniesienia skargi do właściwego organu krajowego wyznaczonego zgodnie z art. 37 aktu w sprawie danych ani prawa którejkolwiek ze stron do skorzystania ze skutecznego środka ochrony prawnej przed sądem w państwie członkowskim.

13.6.3. [WARIANT – jeżeli użytkownik jest przedsiębiorstwem] [Sądy (*określić państwo członkowskie*) będą miały wyłączną właściwość do rozpoznania sprawy dotyczącej niniejszej umowy.]

Dodatek 1

Szczegółowe informacje dotyczące danych objętych niniejszą umową oraz ustaleń dotyczących dostępu

W tym dodatku strony powinny podać szczegółowe informacje dotyczące danych objętych niniejszą umową, ustaleń dotyczących dostępu oraz środków i informacji niezbędnych do uzyskania dostępu do danych i ich wykorzystywania, zgodnie z klauzulami 2 i 3.

A. **Specyfikacja treści danych**

W dodatku należy w pierwszej kolejności uporządkować i wyszczególnić objęte umową dane z produktu oraz dane z usługi powiązanej, wraz ze wskazaniem treści danych oraz częstotliwości ich gromadzenia, tak aby poinformować użytkownika w sposób precyzyjny o informacjach zawartych w tych danych (ustrukturyzowany wykaz punktów danych lub precyzyjne kategorie danych).

B. **Okres zatrzymywania danych**

Następnie w dodatku należy wskazać okres zatrzymywania, tak aby poinformować użytkownika o czasie dostępności danych. Można to zrobić w sposób szczegółowy w odniesieniu do każdego punktu danych lub każdej grupy punktów danych.

C. **Szczegółowe uregulowania dotyczące danych**

W dodatku powinno być określone, czy całość lub część danych stanowi dane objęte szczegółowymi uregulowaniami. Można np. wskazać, czy i jakie dane kwalifikują się jako dane osobowe.

D. **Struktura i format danych**

W dodatku powinno być określone, w jakim ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego udostępnia się dane.

E. **Polityka dostępu**

Może się zdarzyć, że użytkownik przeniesie swoje prawa do korzystania z produktu lub otrzymywania usług powiązanych na kolejnego użytkownika lub że wielu użytkowników współdzieli te prawa. W takich przypadkach strony powinny określić w tym miejscu prawa dostępu do danych w przypadku przeniesienia prawa do korzystania z produktu lub w przypadku istnienia wielu użytkowników. Dodatek może w szczególności zawierać wykaz:

— danych usuwalnych przez użytkownika – produkty lub usługi powiązane często umożliwiają użytkownikowi usunięcie danych wygenerowanych podczas korzystania z tych produktów lub usług. W przypadku przeniesienia prawa do korzystania użytkownik powinien usunąć takie dane. W przeciwnym razie takie dane mogą być dostępne dla kolejnego użytkownika;

— danych zawsze usuwalnych – danych, których posiadacz danych nie powinien udostępniać kolejnemu użytkownikowi;

— pozostałych danych – danych innych niż dane usuwalne przez użytkownika lub dane zawsze usuwalne; takie dane nie będą usuwalne i nie będą podlegać umowie o zachowanie poufności (tj. dane będą również dostępne dla nowych kolejnych użytkowników). Takie dane mogą obejmować dane, które muszą być dostępne dla kolejnego użytkownika z mocy prawa lub w praktyce (na przykład dane związane z aktualizacjami wprowadzanymi w pojeździe podłączonym do internetu.

F. **Nośnik do przekazania danych lub udzielenia dostępu do danych**

W dodatku powinno być wskazane, za pomocą jakiego bezpiecznego nośnika elektronicznego posiadacz danych może udostępnić dane użytkownikowi w drodze przekazania albo udzielenia dostępu.

G. **Informacje niezbędne do wykonywania praw dostępu przysługujących użytkownikowi**

W tym miejscu w dodatku można określić informacje, które są niezbędne do wykonywania praw dostępu przysługujących użytkownikowi. Mogą one obejmować dane osoby wyznaczonej do kontaktów w celu rozwiązywania problemów technicznych zarówno po stronie posiadacza danych, jak i po stronie użytkownika.

Dodatek 2

Treść wniosku użytkownika o dostęp do danych

Poniżej przedstawiono formularz jednego konkretnego wniosku. Można tu uwzględnić wiele różnych wniosków, co jest zalecane na przykład w celu segmentacji określonych przepływów danych, tak aby można było nimi zarządzać oddzielnie, w podziale na poszczególne przepływy danych, poszczególne cele oraz etapy cyklu życia danych (na przykład w przypadku przepływów danych osobowych lub podobnych).

Chociaż w poniższym formularzu wymieniono kluczowe elementy wniosku, można go dostosować, w szczególności na potrzeby procedur elektronicznych.

Dane identyfikacyjne użytkownika	Imię i nazwisko/nazwa: określić Nr umowy: *określić*
Dane identyfikacyjne osoby składającej wniosek w imieniu użytkownika (w stosownych przypadkach)	Imię i nazwisko/nazwa: określić Relacja z użytkownikiem: *określić* Załączyć dowód umocowania do działania w imieniu użytkownika.
Produkty lub usługi, których dotyczy wniosek	Produkt/usługa 1: określić (np. numer seryjny) Produkt/usługa 2: określić (np. numer seryjny)
Punkty danych, których dotyczy wniosek	☐ Wszystkie dane, które są łatwo dostępne posiadaczowi danych ☐ Inne: określić punkty danych objęte wnioskiem
Charakter danych, których dotyczy wniosek	☐ Obejmujące dane osobowe Jeżeli użytkownik nie jest osobą, której dane dotyczą, należy podać ważną podstawę prawną przetwarzania zgodnie z art. 6 rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, sposób spełnienia warunków określonych w art. 9 tego rozporządzenia i art. 5 ust. 3 dyrektywy 2002/58/WE. ☐ Tylko dane nieosobowe
Data danych, których dotyczy wniosek	☐ Dane z przeszłości: wskazać okres ☐ Przyszłe dane: wskazać okres
Czas dostępu do danych (w zależności od tego, co określono w dodatku 1)	☐ W sposób ciągły ☐ W czasie rzeczywistym ☐ Inne: określić
Sposób dostępu do danych (w zależności od tego, co określono w dodatku 1)	☐ Przekazanie danych ☐ Dostęp do danych w miejscu ich przechowywania
Miejsce docelowe przekazania danych:	określić w zależności od odpowiedzi na poprzedni punkt
Data wniosku	określić

Dodatek 3

Formularz wniosku użytkownika o udostępnienie danych osobie trzeciej

Poniżej przedstawiono formularz jednego konkretnego wniosku. Można tu uwzględnić wiele różnych wniosków, co jest zalecane na przykład w celu segmentacji określonych przepływów danych, tak aby konkretny odbiorca danych wyznaczony przez użytkownika mógł zarządzać poszczególnymi przepływami danych oddzielnie, w podziale na poszczególne przepływy danych oraz cele.

Dane identyfikacyjne użytkownika	Imię i nazwisko/nazwa: określić Nr umowy: *określić*
Dane identyfikacyjne osoby składającej wniosek w imieniu użytkownika (w stosownych przypadkach)	Imię i nazwisko/nazwa: określić Relacja z użytkownikiem: *określić*
Produkty lub usługi, których dotyczy wniosek	Produkt/usługa 1: *określić* Produkt/usługa 2: *określić*
Dane, których dotyczy wniosek Uwaga: nie ma zastosowania w kontekście testowania nowych produktów skomunikowanych, substancji lub procesów, które nie zostały jeszcze wprowadzone do obrotu.	☐ Wariant 1: wszystkie dane, które są łatwo dostępne posiadaczowi danych ☐ Wariant 2: określić, zgodnie z dodatkiem 1 do umowy między użytkownikiem a odbiorcą danych, dane, które mają być udostępniane odbiorcy danych ☐ Wariant 3: określone przez odbiorcę danych w dodatku 2 do umowy między posiadaczem danych a odbiorcą danych
Jeżeli dane obejmują dane osobowe	Podać ważną podstawę prawną przetwarzania zgodnie z art. 6 rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, sposób spełnienia warunków określonych w art. 9 tego rozporządzenia i art. 5 ust. 3 dyrektywy 2002/58/WE
Dane identyfikacyjne osoby trzeciej Uwaga: taka osoba trzecia nie może być strażnikiem dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925.	Imię i nazwisko/nazwa: określić Dane kontaktowe: *określić*

Dodatek 4

Szczegółowe informacje na temat środków ochrony tajemnic przedsiębiorstwa

(do opracowania przez strony)

[WARIANT] Dodatek 5

Szczegółowe informacje na temat dzielenia się danymi z osobami trzecimi

(do opracowania przez strony)

Dodatek 6

Szczegółowe informacje na temat środków ochrony

(do opracowania przez strony)

[WARIANT] Dodatek 7

Szczegółowe informacje na temat rekompensaty dla użytkownika

(do opracowania przez strony)

[WARIANT] Dodatek 8

Szczegółowe informacje na temat kar

(do opracowania przez strony)

[WARIANT] Dodatek 9

Dokumentacja dotycząca własności produktu lub praw umownych do korzystania z produktu lub usług powiązanych

(dokumentacja do załączenia przez strony)

[WARIANT] Dodatek 10

Szczegółowe informacje na temat ustaleń dotyczących dostępu dodatkowych użytkowników do danych

(do opracowania przez strony)

ZAŁĄCZNIK III

MODELOWE POSTANOWIENIA UMOWNE

na potrzeby umów między użytkownikami a odbiorcami danych

Poniższe modelowe postanowienia umowne opracowano na potrzeby umów między użytkownikiem produktu skomunikowanego lub usługi powiązanej a odbiorcą danych, z którym użytkownik musi lub chce dzielić się danymi na podstawie art. 5 rozporządzenia (UE) 2023/2854 (zwanego dalej „aktem w sprawie danych").

Główną nowością wprowadzoną przez akt w sprawie danych w tym zakresie jest to, że:

— użytkownik może zobowiązać posiadacza danych do dzielenia się danymi z wybranym przez użytkownika odbiorcą danych;

— użytkownik określa w umowie z odbiorcą danych, do jakich celów i na jakich warunkach odbiorca danych może wykorzystywać dane i dzielić się danymi;

— nieuczciwe postanowienia umowne dotyczące dostępu do danych i ich wykorzystywania lub odpowiedzialności i środków ochrony prawnej wobec naruszenia lub odstąpienia od obowiązków dotyczących danych nie są wiążące, jeżeli zostały nałożone na przedsiębiorstwo jednostronnie przez inne przedsiębiorstwo.

Taka umowa często następuje po umowie zawartej między posiadaczem danych a użytkownikiem i poprzedza umowę, która również musi zostać zawarta między posiadaczem danych a odbiorcą danych.

Umowa ma strukturę modułową i chociaż mogłaby istnieć jako samodzielna umowa w przypadku zastosowania wszystkich klauzul (gdy dzielenie się danymi stanowi główny cel umowy), strony mogą również wybrać wyłącznie te klauzule, które pasują do ich konkretnej sytuacji. Jeżeli dzielenie się danymi stanowi jedynie warunek wstępny wykonania umowy zawartej w innym celu, np. umowy dotyczącej naprawy i konserwacji maszyny przemysłowej, wystarczające mogłoby być zastosowanie klauzul 1.2, 1.3, 2, 3 i 4 (z wyjątkiem klauzuli 4.1.1 lit. b)), ponieważ treść pozostałych klauzul niniejszej umowy prawdopodobnie byłaby objęta umową dotyczącą naprawy i konserwacji.

1. Strony i produkt/usługi powiązane

1.1. Strony umowy

Niniejsza umowa o dostępie do danych i ich wykorzystywaniu zostaje zawarta między

(wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia) („użytkownik")

a

(wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia) („odbiorca danych")

zwanymi w niniejszej umowie łącznie „stronami", a każdy indywidualnie „stroną".

„**Użytkownik**" oznacza osobę fizyczną lub prawną, która jest właścicielem produktu skomunikowanego lub której na podstawie umowy przekazane zostały tymczasowe prawa do korzystania z tego produktu skomunikowanego, lub która korzysta z usług powiązanych.

„**Odbiorca danych**" to osoba trzecia wybrana przez użytkownika. Może nim być osoba fizyczna albo prawna działająca w celach związanych z jej działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, inna niż użytkownik produktu skomunikowanego lub usługi powiązanej, której to osobie posiadacz danych udostępnia dane, w tym osoba trzecia na wniosek użytkownika skierowany do posiadacza danych lub zgodnie z obowiązkiem prawnym wynikającym z prawa Unii lub prawa krajowego przyjętego zgodnie z prawem Unii.

Taki odbiorca danych może konkurować z posiadaczem danych. Strażnik dostępu nie kwalifikuje się jednak do bycia lub stania się odbiorcą danych.

1.2. Kwalifikowalność odbiorcy danych

Odbiorca danych oświadcza, że nie został wskazany jako strażnik dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925 ([1]) („akt o rynkach cyfrowych").

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. L 265 z 12.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

1.3. **Wniosek do posiadacza danych i współpraca stron**

1.3.1. Strony postanawiają, że:

[WARIANT 1] [użytkownik wystąpi do

(*wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia*) („posiadacz danych")

z wnioskiem o udostępnienie odbiorcy danych danych określonych w klauzuli 2.]

[WARIANT 2] [użytkownik upoważnia odbiorcę danych do wystąpienia w imieniu użytkownika do

(*wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia*) („posiadacz danych")

z wnioskiem o udostępnienie odbiorcy danych danych określonych w klauzuli 2.]

1.3.2. Użytkownik i odbiorca danych będą współpracować w dobrej wierze w celu zapewnienia odpowiedniego kontaktu i współdziałania z posiadaczem danych. W szczególności odbiorca danych zawrze z posiadaczem danych odrębną umowę („umowa między posiadaczem danych a odbiorcą danych"), [WARIANT: w ścisłym porozumieniu z użytkownikiem] i zgodnie z mającym zastosowanie prawem, w tym między innymi z aktem w sprawie danych. Odbiorca danych musi zapewnić zgodność umowy między posiadaczem danych a odbiorcą danych z niniejszą umową.

1.3.3. Niniejszą umowę zawiera się w odniesieniu do:

a) następujących produktów skomunikowanych („produkt"): (*wstawić nazwę i dalsze specyfikacje konkretnego produktu skomunikowanego objętego umową*);

b) następujących usług powiązanych („usługi powiązane"): (*w stosownych przypadkach wstawić nazwę oraz dalsze specyfikacje konkretnych usług powiązanych lub rodzaju usług powiązanych objętych umową*).

Użytkownik oświadcza, że jest właścicielem produktu albo jest uprawniony do używania produktu na podstawie umowy najmu, dzierżawy, leasingu lub podobnej umowy lub do otrzymywania usług powiązanych na podstawie umowy o świadczenie usług.

[WARIANT 1] [Użytkownik zobowiązuje się do przekazania odbiorcy danych, na należycie uzasadniony wniosek, wszelkich istotnych dokumentów na potwierdzenie tego oświadczenia, jeżeli zajdzie taka potrzeba.]

[WARIANT 2] [Dokumentacja potwierdzająca to oświadczenie, a także informacje dotyczące tego, kogo należy uznać za użytkownika na potrzeby niniejszej umowy, zostały określone w **dodatku 5**.]

2. **Dane objęte umową**

Dane objęte niniejszą umową obejmują wszystkie łatwo dostępne dane z produktu lub usług powiązanych wygenerowane w wyniku korzystania z produktu lub usług powiązanych:

[WARIANT 1] [w rozumieniu aktu w sprawie danych.]

[WARIANT 2] [w rozumieniu aktu w sprawie danych, wymienione w dodatku 1.]

[WARIANT 3] [w rozumieniu aktu w sprawie danych, w zakresie niezbędnym do celów uzgodnionych w klauzuli 3 oraz dodatkowo wymienionych przez odbiorcę danych w dodatku 2 do umowy między posiadaczem danych a odbiorcą danych.]

Użytkownik nie ponosi odpowiedzialności za jakość, charakterystykę i ilość danych, ani za ich przydatność do określonego celu.

Zgodnie z aktem w sprawie danych „**dane z produktu**” oznaczają dane wygenerowane w wyniku korzystania z produktu skomunikowanego, które producent zaprojektował tak, by użytkownik, posiadacz danych lub osoba trzecia, w tym w stosownym przypadku producent, mogli je pobierać za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu.

„**Dane z usług powiązanych**” oznaczają dane stanowiące cyfrowe odwzorowanie czynności lub zdarzeń z udziałem użytkownika związanych z produktem skomunikowanym, utrwalane przez użytkownika celowo lub generowane jako produkt uboczny jego czynności, podczas świadczenia usługi powiązanej przez dostawcę.

Dane z produktu i usług powiązanych mogą być zarówno danymi osobowymi, jak i nieosobowymi.

„**Dane łatwo dostępne**” obejmują „dane z produktu i dane z usługi powiązanej, które posiadacz danych zgodnie z prawem pozyskuje lub może zgodnie z prawem pozyskać z produktu skomunikowanego lub z usługi powiązanej bez nieproporcjonalnie dużego wysiłku wykraczającego poza prostą czynność”.

Jak wyjaśniono w motywach, definicja ta nie obejmuje „danych generowanych w wyniku korzystania z produktu skomunikowanego, jeżeli projekt produktu skomunikowanego nie przewiduje przechowywania lub przesyłania takich danych poza elementem składowym, w którym są one generowane, lub poza całym produktem” (motyw 20). „O tym, jakie dane jest w stanie udostępniać produkt skomunikowany, powinny decydować wybory projektowe producenta oraz w stosownym przypadku prawo Unii lub prawo krajowe uwzględniające potrzeby i cele danego sektora lub stosowne decyzje właściwych organów” (motyw 14).

3. Wykorzystywanie danych przez odbiorcę danych

Umowy w sprawie dzielenia się danymi między użytkownikami a odbiorcami danych mogą na przykład ustanawiać nowy stosunek prawny lub stanowić uzupełnienie istniejącego stosunku między stronami, niezależnie od tego, czy dotyczą dzielenia się danymi w celach komercyjnych, czy nie. Umowy takie powinny mieć charakter niewyłączny, z wyjątkiem przypadków o ściśle określonym zakresie, ograniczonych do konkretnych danych, rynku, celu i okresu obowiązywania oraz dobrze wynagradzanych.

3.1. Uzgodnione wykorzystywanie danych

To do użytkownika należy rozważenie, z której części jego danych i w jakim celu odbiorca danych będzie mógł korzystać, a w szczególności – w jakim zakresie odbiorca danych powinien mieć możliwość dzielenia się danymi z innymi osobami trzecimi.

Na przykład użytkownik może zwrócić się do odbiorcy danych o monitorowanie funkcjonowania produktu lub usługi powiązanej i o działanie jako pośrednik przekazujący sprzedawcy sprzętu zgłoszenia roszczeń gwarancyjnych w imieniu użytkownika.

Użytkownik powinien również rozważyć, czy zezwolić odbiorcy danych na dzielenie się danymi z podmiotami komercyjnymi lub niekomercyjnymi. Dzielenie się danymi w celach niekomercyjnych może obejmować dzielenie się danymi i wykorzystywanie danych z pobudek altruistycznych lub z innych powodów, bez nastawienia na zysk, do celów leżących w interesie publicznym, badań naukowych, statystycznych lub innych badań analitycznych (jeżeli ma to zastosowanie i jest wymagane lub nie ma zastosowania ani nie jest wymagane, ale jest przewidziane zgodnie z art. 89 RODO, dyrektywą w sprawie otwartych danych (UE) 2019/1024, rozporządzeniem w sprawie zbiorów danych o wysokiej wartości (UE) 2023/138, aktem w sprawie zarządzania danymi (UE) 2022/868, rozporządzeniem w sprawie przestrzeni danych dotyczących zdrowia (UE) 2025/327 itp.) przez odbiorcę danych lub za jego pośrednictwem z odpowiednimi społecznościami, gminami, regionami, narodami, organizacjami pozarządowymi i innymi organizacjami niekomercyjnymi. W przypadku dzielenia się danymi w celach komercyjnych zaleca się, aby nie odnosić się do terminu „sprzedaż” ani nie stosować go, ponieważ dla niektórych zainteresowanych stron może on sugerować przeniesienie tytułu prawnego lub kontroli nad danymi lub ich przekazanie odbiorcy danych na wyłączność. Nie jest to potrzebne ani zalecane, zwłaszcza że dane są zarówno aktywem cyfrowym, jak i środkiem cyfrowym i mogą być wykorzystywane do wielu celów w całym cyklu życia danych – nawet do wielu celów komercyjnych – przy jednoczesnym zapewnieniu odbiorcy danych przewagi rynkowej lub innego tworzenia wartości, co również uzasadnia godziwe wynagrodzenie dla użytkownika za udzielenie takiej licencji na (ponowne) wykorzystywanie danych.

Użytkownik powinien ocenić konsekwencje przyznania odbiorcy danych prawa do wykorzystywania danych oraz – w stosownych przypadkach – dzielenia się danymi, a także rozważyć, czy prawa te powinny być przyznane w zamian za rekompensatę.

3.1.1. Odbiorca danych może wykorzystywać dane wyłącznie do następujących celów, które nie mogą być sprzeczne z praktykami wymienionymi w klauzuli 3.2: *(wstawić uzgodnione cele)*.

Przykłady uzgodnionych celów wykorzystywania danych przez odbiorcę danych:

— świadczenie na rzecz użytkownika regularnych usług konserwacji lub usług rynku posprzedażowego dotyczących produktu;

— prowadzenie badań w określonych dziedzinach;

— opracowywanie nowych usług lub ulepszanie, modernizacja lub utrzymywanie produktów lub usług, w tym rozwiązań w zakresie AI;

— agregowanie danych z innymi danymi lub tworzenie danych wywnioskowanych w dowolnym zgodnym z prawem celu, w tym w celu sprzedaży lub udostępnienia w inny sposób takich zagregowanych lub wywnioskowanych danych osobom trzecim.

3.1.2. Odbiorca danych musi usunąć dane, gdy nie są już one potrzebne do uzgodnionych celów.

3.2. **Nieuprawnione wykorzystywanie danych**

Odbiorca danych nie może wykorzystywać danych:

a) do jakiegokolwiek celu innego niż cele uzgodnione w klauzuli 3.1;

b) do jakiegokolwiek celu, który narusza prawo Unii lub mające zastosowanie prawo krajowe;

c) do profilowania osób fizycznych w rozumieniu art. 4 pkt 4 RODO, chyba że jest to niezbędne do świadczenia usługi żądanej przez użytkownika;

d) do opracowania produktu, który konkuruje z produktem objętym niniejszą umową;

e) do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji użytkownika lub na temat korzystania przez użytkownika z produktu lub usługi powiązanej w jakikolwiek sposób, który mógłby osłabić pozycję handlową użytkownika na rynkach, na których prowadzi on działalność, chyba że użytkownik udzielił zgody na takie wykorzystywanie;

f) w sposób, który negatywnie wpływa na bezpieczeństwo produktu lub jakiejkolwiek usługi powiązanej;

g) [WARIANT] [do innych celów: *(określić w szczególności zastosowania, które* w znacznym stopniu szkodzą prawnie uzasadnionym interesom użytkownika)].

3.3. **Wykorzystywanie danych osobowych przez odbiorcę danych**

Odbiorca danych wykorzystuje lub w inny sposób przetwarza wszelkie dane będące danymi osobowymi wyłącznie wówczas, gdy istnieje ku temu podstawa prawna, oraz przy spełnieniu warunków ustanowionych w rozporządzeniu (UE) 2016/679 (RODO) oraz – w stosownych przypadkach – dyrektywie 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej).

Regulując kwestię przetwarzania danych osobowych zgodnie z mającymi zastosowanie przepisami o ochronie danych (w tym między innymi z rozporządzeniem (UE) 2016/679), strony muszą rozważyć, czy użytkownik jest osobą, której dane dotyczą, w odniesieniu do całości lub części danych osobowych zawartych w danych objętych umową.

3.4. **Stosowanie środków ochrony**

Odbiorca danych zobowiązuje się stosować w celu zapobiegania utracie danych oraz nieuprawnionemu dostępowi do danych środki ochrony, [WARIANT 1] [które są zasadne w danych okolicznościach, z uwzględnieniem aktualnego stanu wiedzy naukowej i technicznej, potencjalnej szkody poniesionej przez użytkownika oraz kosztów związanych ze stosowaniem środków ochrony.] [WARIANT 2] [które zostały szczegółowo określone w **dodatku 2**.]

Strony powinny rozważyć, czy chcą zawrzeć w oddzielnym dodatku wszystkie szczegółowe informacje na temat tego, w jaki sposób można skutecznie chronić ważne interesy użytkownika. Środki mogą mieć zarówno charakter techniczny (np. szyfrowanie, zapory sieciowe, przechowywanie danych w odrębnych lokalizacjach), jak i organizacyjny (np. zaangażowanie zaufanej osoby trzeciej). Ponieważ środki muszą być proporcjonalne, ich treść będzie się znacznie różnić w zależności od charakteru danych i wchodzących w grę interesów.

4. **Dzielenie się danymi z osobami trzecimi i korzystanie z usług przetwarzania danych**

Zgodnie z art. 6 ust. 2 lit. c) aktu w sprawie danych odbiorca danych „nie udostępnia otrzymanych danych innej osobie trzeciej, chyba że udostępnia je na podstawie umowy z użytkownikiem, i pod warunkiem że ta inna osoba trzecia zastosuje wszystkie niezbędne środki uzgodnione między posiadaczem danych a osobą trzecią w celu ochrony poufności tajemnic przedsiębiorstwa".

W związku z tym, jeżeli użytkownik zdecyduje się przyznać to prawo odbiorcy danych, klauzulę tę należy włączyć do umowy, ewentualnie przewidując rekompensatę.

4.1. **Warunki dzielenia się danymi**

4.1.1. Odbiorca danych może dzielić się danymi będącymi danymi nieosobowymi z osobami trzecimi, jeżeli spełnione są następujące warunki:

a) dane te są wykorzystywane przez osobę trzecią wyłącznie do następujących celów:

(i) wspierania odbiorcy danych w osiąganiu celów uzgodnionych w klauzuli 3.1;

(ii) osiągania, we współpracy z odbiorcą danych lub za pośrednictwem spółek celowych, celów uzgodnionych w klauzuli 3.1 oraz

(iii) [WARIANT] [(*określić szczegółowe cele, do których osoby trzecie mogą dążyć na własne potrzeby, niezależnie od odbiorcy danych, oraz czy dzielenie się danymi do tych celów następuje odpłatnie czy nieodpłatnie*) oraz]

b) dana osoba trzecia nie została wskazana jako strażnik dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925 („akt o rynkach cyfrowych") oraz

c) odbiorca danych zobowiązuje osobę trzecią umownie do:

(i) niewykorzystywania danych do celów innych niż cele uzgodnione w klauzuli 4.1.1 lit. a);

(ii) niepozyskiwania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji użytkownika lub na temat korzystania przez użytkownika z produktu lub usługi powiązanej w jakikolwiek inny sposób, który mógłby osłabić pozycję handlową użytkownika na rynkach, na których prowadzi on działalność;

(iii) niewykorzystywania danych w sposób, który w inny sposób znacząco szkodzi prawnie uzasadnionym interesom użytkownika, w szczególności gdy takie dane zawierają szczególnie chronione dane handlowe lub są chronione tajemnicami przedsiębiorstwa lub prawami własności intelektualnej;

(iv) stosowania środków ochrony wymaganych na mocy klauzuli 3.4 oraz

(v) skasowania danych, gdy nie będą już one niezbędne do celów uzgodnionych w klauzuli 4.1.1 lit. a);

(vi) niedzielenia się tymi danymi dalej.

4.1.2. Dalsze szczegółowe informacje, w tym te dotyczące tożsamości osób trzecich, ograniczeń w zakresie wykorzystywania danych przez osoby trzecie, a także dalszych warunków i środków ochrony, przedstawiono szczegółowo w **dodatku 3**.

4.1.3. Niezależnie od klauzul od 4.1.1 do 4.1.2 odbiorca danych może – na własny rachunek i na własną odpowiedzialność – korzystać z usług przetwarzania danych, np. usług przetwarzania w chmurze (w tym infrastruktury jako usługi, platformy jako usługi i oprogramowania jako usługi), usług hostingu lub podobnych usług, w celu osiągnięcia uzgodnionych celów określonych w klauzuli 3.2.1 lit. a). Osoby trzecie mogą również – na własny rachunek i na własną odpowiedzialność – korzystać z takich usług w celu osiągnięcia uzgodnionych celów określonych w klauzuli 4.1.1 lit. a). Odbiorca danych dzieli się z osobami trzecimi wszelkimi danymi będącymi danymi osobowymi lub w inny sposób przetwarza takie dane wyłącznie wówczas, gdy istnieje ku temu podstawa prawna oraz przy spełnieniu warunków dopuszczonych na mocy rozporządzenia (UE) 2016/679 (RODO) oraz – w stosownych przypadkach – dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej).

5. **Rekompensata**

Odbiorca danych zobowiązuje się do wypłacenia użytkownikowi rekompensaty, jak określono szczegółowo w **dodatku 4**.

Strony mogą uzgodnić rekompensatę za wykorzystywanie danych i dzielenie się danymi przez odbiorcę danych, jeżeli uznają to za sprawiedliwe i zasadne. Mogą na przykład rozważyć taką rekompensatę w sytuacji, gdy odbiorca danych wykorzystuje dane do opracowywania nowych produktów lub usług lub gdy odbiorca danych tworzy dane zagregowane lub wywnioskowane do celów komercyjnych. Natomiast w przypadku, gdy na przykład dane są wykorzystywane wyłącznie na potrzeby jakiejkolwiek umowy zawartej z użytkownikiem, umowa może nie przewidywać rekompensaty.

Podobnie w celu zapewnienia sprawiedliwego traktowania użytkownika rekompensata może być potrzebna, jeżeli użytkownik zgadza się na to, by odbiorca danych mógł sprzedawać dane osobom trzecim zgodnie z klauzulą 4.1.1 lit. a) pkt (iii). Jeżeli rekompensata jest należna, strony muszą uzgodnić jej charakter, który może mieć formę pieniężną lub niepieniężną.

6. **Data rozpoczęcia stosowania, okres obowiązywania i rozwiązanie umowy**

6.1. **Data rozpoczęcia stosowania i okres obowiązywania**

6.1.1. Niniejsza umowa [WARIANT 1] [wchodzi w życie ze skutkiem natychmiastowym] [WARIANT 2] [wchodzi w życie z dniem (*wskazać datę*)].

6.1.2. [WARIANT] [Niniejsza umowa zostaje zawarta [WARIANT 1] [na czas nieokreślony] [WARIANT 2] [na czas określony (wskazać)], z zastrzeżeniem wszelkich podstaw do jej wygaśnięcia lub rozwiązania przewidzianych w niniejszej umowie.]

6.2. **Rozwiązanie umowy**

6.2.1. Odbiorca danych może rozwiązać niniejszą umowę przez złożenie użytkownikowi wypowiedzenia z zachowaniem (*wskazać okres wypowiedzenia*) okresu wypowiedzenia, jeżeli umowa między posiadaczem danych a odbiorcą danych została rozwiązana.

6.2.2. Jeżeli użytkownik utraci status użytkownika, niniejsza umowa ulega rozwiązaniu. Użytkownik składa odbiorcy danych wypowiedzenie z zachowaniem (*wskazać okres wypowiedzenia*) okresu wypowiedzenia.

6.2.3. [WARIANT – w przypadku umowy zawartej na czas nieokreślony lub gdy strony chcą dopuścić rozwiązanie umowy bez podania przyczyny] [Każda ze stron może rozwiązać niniejszą umowę w dowolnym momencie przed rozpoczęciem jej obowiązywania lub w okresie jej obowiązywania, składając drugiej stronie wypowiedzenie z zachowaniem (*wskazać okres wypowiedzenia*) okresu wypowiedzenia.] [WARIANT] Jeżeli użytkownik wypowie niniejszą umowę na podstawie tej klauzuli przed *(wstawić moment w czasie lub minimalny okres obowiązywania umowy)*, użytkownik zapłaci drugiej stronie rekompensatę za koszty poniesione w związku z realizacją niniejszej umowy, w następujący sposób: *(określić odpowiednio)*.

W przypadkach, w których użytkownik jest umownie zobowiązany do dzielenia się danymi z odbiorcą danych, klauzula ta nie powinna być stosowana, ponieważ mogłoby to prowadzić do naruszenia innej umowy.

6.3. **Skutki wygaśnięcia lub rozwiązania umowy**

6.3.1. Wygaśnięcie okresu obowiązywania umowy lub rozwiązanie niniejszej umowy zwalnia obie strony z zobowiązania do wykonania oraz do przyjęcia przyszłego świadczenia, lecz nie wpływa na prawa i zobowiązania, które powstały do chwili wygaśnięcia lub rozwiązania umowy.

Wygaśnięcie lub rozwiązanie umowy nie ma wpływu na żadne postanowienie, które ma obowiązywać nawet po wygaśnięciu umowy, w szczególności na wszelkie ograniczenia dotyczące dopuszczalnego wykorzystywania danych i dzielenia się danymi przez odbiorcę danych na podstawie klauzul 3 i 4, klauzuli 8.1 – dotyczącej poufności, klauzuli 8.3 – dotyczącej prawa właściwego, oraz klauzuli 8.6 – dotyczącej rozstrzygania sporów.

6.3.2. W szczególności rozwiązanie lub wygaśnięcie umowy wywołuje następujące skutki:

a) odbiorca danych zaprzestaje pobierania wygenerowanych lub zarejestrowanych danych niezwłocznie z dniem rozwiązania lub wygaśnięcia umowy;

b) [WARIANT] odbiorca danych zachowuje prawo do wykorzystywania danych i dzielenia się danymi, które zostały wygenerowane lub zarejestrowane przed datą rozwiązania lub wygaśnięcia określonymi w klauzulach 3 i 4 [WARIANT – przez okres *(wskazać okres)*].

Mogą wystąpić przypadki, w których odbiorca danych musi ponieść nakłady inwestycyjne w związku z dzieleniem się danymi, na przykład przez dostosowanie swojej infrastruktury cyfrowej; nakłady te są amortyzowane w czasie. W takim przypadku strony mogą chcieć zapewnić, aby odbiorca danych otrzymał rekompensatę od strony rozwiązującej umowę. Wysokość rekompensaty powinna pozostawać do ustalenia.

7. Środki ochrony prawnej w przypadku niewykonania zobowiązania

7.1. Przypadki niewykonania zobowiązania

7.1.1. Niewykonanie zobowiązania przez stronę jest istotnym naruszeniem zobowiązania, jeżeli:

a) niewykonanie zobowiązania w znacznym stopniu pozbawia drugą stronę tego, czego miała prawo oczekiwać na podstawie niniejszej umowy, chyba że strona, która nie wykonała zobowiązania, nie przewidziała i nie mogła w rozsądny sposób przewidzieć takiego rezultatu, lub

b) z okoliczności jasno wynika, że nie można polegać na przyszłym wykonaniu zobowiązań przez stronę, która nie wykonała zobowiązania.

7.1.2. Niewykonanie zobowiązania przez stronę jest usprawiedliwione, jeżeli wynika z przeszkody pozostającej poza jej kontrolą oraz jeżeli nie można było w rozsądny sposób oczekiwać, aby w chwili zawarcia niniejszej umowy strona ta uwzględniła tę przeszkodę bądź jej uniknęła lub przezwyciężyła ją lub jej skutki.

7.1.3. Jeżeli przeszkoda jest tylko tymczasowa, niewykonanie zobowiązania przez stronę jest usprawiedliwione tylko w okresie, w którym istnieje przeszkoda. Jeżeli jednak opóźnienie stanowi istotne naruszenie zobowiązania, druga strona może je tak traktować.

Strona, która nie wykonała zobowiązania, ma obowiązek dopilnować, aby zawiadomienie o przeszkodzie oraz jej wpływie na możliwość wykonania zobowiązania dotarło do drugiej strony bez zbędnej zwłoki po tym, jak strona, która nie wykonała zobowiązania, dowiedziała się lub powinna była się dowiedzieć o tych okolicznościach. Druga strona jest uprawniona do odszkodowania za szkodę ekonomiczną wynikłą z nieotrzymania takiego zawiadomienia.

7.2. Środki ochrony prawnej w przypadku niewykonania zobowiązania

7.2.1. W przypadku niewykonania zobowiązania przez jedną ze stron drugiej stronie przysługują środki ochrony prawnej wymienione w poniższych klauzulach, bez uszczerbku dla wszelkich środków ochrony prawnej dostępnych na podstawie prawa właściwego.

7.2.2. Dopuszczalne jest łączenie środków ochrony prawnej, które wzajemnie się nie wykluczają.

7.2.3. Strona nie może skorzystać ze środka ochrony prawnej w zakresie, w jakim sama spowodowała niewykonanie zobowiązania przez drugą stronę, na przykład gdy uchybienie w jej własnej infrastrukturze danych uniemożliwiło drugiej stronie należyte wykonanie jej zobowiązań. Strona nie może również powoływać się na roszczenie odszkodowawcze z tytułu poniesionych szkód w zakresie, w jakim mogła ograniczyć powstałą szkodę przez podjęcie zasadnych kroków.

7.2.4. Strona poszkodowana może:

a) rozwiązać niniejszą umowę ze skutkiem natychmiastowym i bez ponoszenia kar, w drodze wypowiedzenia złożonego drugiej stronie, jeżeli:

(i) niewykonanie zobowiązania przez drugą stronę stanowi istotne naruszenie zobowiązania lub

(ii) w przypadku niewykonania, które nie stanowi istotnego naruszenia zobowiązania, strona poszkodowana przekazała zawiadomienie wyznaczające rozsądny termin na usunięcie uchybienia, a termin ten upłynął bez wykonania zobowiązania przez drugą stronę;

b) dochodzić odszkodowania za szkodę ekonomiczną poniesioną w wyniku niewykonania zobowiązania przez drugą stronę, jeżeli to niewykonanie nie jest usprawiedliwione na mocy klauzuli 7.1.2. Strona, która nie wykonała zobowiązania, ponosi odpowiedzialność wyłącznie za szkodę, którą przewidywała lub którą mogła w rozsądny sposób przewidzieć w chwili zawarcia niniejszej umowy jako prawdopodobny skutek niewykonania zobowiązania, chyba że niewykonanie zobowiązania miało charakter umyślny lub stanowiło rażące zaniedbanie;

c) żądać, aby strona, która nie wykonała zobowiązania, bez zbędnej zwłoki wykonała swoje zobowiązania wynikające z niniejszej umowy, chyba że byłoby to niezgodne z prawem lub niemożliwe lub wykonanie zobowiązania powodowałoby dla strony, która nie wykonała zobowiązania, koszty niewspółmierne do korzyści, jakie uzyskałaby druga strona; [WARIANT] [w przypadku gdy strona nie wykona swoich zobowiązań wynikających z niniejszej umowy, jest ona w każdym przypadku zobowiązana do zapłaty kar umownych określonych szczegółowo w dodatku 6, które strony uznają za odszkodowanie w rozumieniu klauzuli 7.2.4 lit. b). stronie, która nie wykonała zobowiązania, przysługuje prawo żądania obniżenia kary do rozsądnej wysokości, jeżeli strona ta wykaże, że kara jest rażąco wygórowana w stosunku do szkody wynikającej z niewykonania zobowiązania.]

8. **Postanowienia ogólne**

8.1. **Poufność**

8.1.1. Następujące informacje muszą być uważane za poufne:

a) informacje odnoszące się do tajemnic przedsiębiorstwa, sytuacji finansowej lub jakiegokolwiek innego aspektu działalności drugiej strony, chyba że dana druga strona sama podała te informacje do publicznej wiadomości;

b) (*w stosownych przypadkach*) informacje określające podstawę obliczenia rekompensaty;

c) informacje odnoszące się do posiadacza danych i każdej innej chronionej osoby trzeciej, chyba że chroniona osoba trzecia podała te informacje do wiadomości publicznej.

8.1.2. Obie strony zgadzają się zastosować wszelkie uzasadnione środki w celu bezpiecznego przechowywania oraz zachowania pełnej poufności informacji, o których mowa w klauzuli 8.1.1, oraz nie ujawniać ani nie udostępniać takich informacji osobom trzecim, chyba że:

a) jedna ze stron jest prawnie zobowiązana do ujawnienia lub udostępnienia odpowiednich informacji lub

b) jedna ze stron musi ujawnić lub udostępnić odpowiednie informacje w celu wypełnienia swoich zobowiązań wynikających z niniejszej umowy, lub

c) jedna ze stron uzyskała uprzednią zgodę drugiej strony lub strony, która przekazała informacje poufne lub której ujawnienie tych informacji dotyczy.

8.1.3. W każdym przypadku użytkownik i odbiorca danych mogą ujawnić lub udostępnić posiadaczowi danych takie informacje, jakie są niezbędne do identyfikacji odbiorcy danych lub użytkownika lub skontaktowania się z nimi w celu zawarcia umowy między posiadaczem danych a odbiorcą danych, o której mowa w klauzuli 1.3.2.

8.1.4. Te zobowiązania do zachowania poufności pozostają w mocy po rozwiązaniu niniejszej umowy przez okres (*wskazać okres*).

8.1.5. Te zobowiązania do zachowania poufności nie znoszą ani nie ograniczają bardziej rygorystycznych obowiązków wynikających z (i) rozporządzenia (UE) 2016/679 (RODO), (ii) przepisów wdrażających dyrektywę 2002/58/WE lub dyrektywę (UE) 2016/943 ani (iii) żadnego innego prawa UE ani prawa państwa członkowskiego.

8.2. **Środki komunikacji**

Wszelkie zawiadomienia lub inne komunikaty wymagane lub dozwolone na mocy niniejszej umowy muszą mieć formę pisemną i mogą być doręczane osobiście, wysyłane pocztą przesyłką opłaconą z góry lub przekazywane drogą elektroniczną, w tym pocztą elektroniczną, pod warunkiem że nadawca zachowa dowód wysłania na adresy wskazane poniżej:

Strona	Osoba wyznaczona do kontaktów	E-mail	Telefon	Adres
Użytkownik	[Imię i nazwisko]/[Stanowisko]	[E-mail]	[Telefon]	[Adres]
Odbiorca danych	[Imię i nazwisko]/[Stanowisko]	[E-mail]	[Telefon]	[Adres]

Każde takie zawiadomienie lub każdy taki komunikat uznaje się za otrzymane:

a) w przypadku doręczenia osobistego – w dniu doręczenia,

b) w przypadku wysłania pocztą przesyłką opłaconą z góry – w trzecim dniu roboczym po dniu nadania,

c) w przypadku przekazania drogą elektroniczną – w dniu przekazania, pod warunkiem że nadawca nie otrzymał żadnego komunikatu o błędzie wskazującego na niedoręczenie.

8.3. **Całość umowy, zmiany i rozdzielność postanowień**

8.3.1. Niniejsza umowa (wraz z dodatkami do niej oraz wszelkimi innymi dokumentami, o których mowa w niniejszej umowie) stanowi całość umowy między stronami w odniesieniu do jej przedmiotu i zastępuje wszelkie wcześniejsze umowy, porozumienia i uzgodnienia stron – zarówno ustne, jak i pisemne – dotyczące przedmiotu niniejszej umowy.

8.3.2. Wszelkie zmiany niniejszej umowy będą ważne wyłącznie wtedy, gdy zostaną uzgodnione przez strony na piśmie, w tym w jakiejkolwiek formie elektronicznej.

8.3.3. Jeżeli którekolwiek postanowienie niniejszej umowy zostanie uznane za nieważne, bezskuteczne, wzruszalne lub niewykonalne z jakiegokolwiek powodu i jeżeli postanowienie to można oddzielić od pozostałych postanowień umowy, te pozostałe postanowienia pozostaną ważne i wykonalne, chyba że danego postanowienia nie można oddzielić od pozostałych postanowień niniejszej umowy. Wszelkie powstałe w ten sposób luki lub niejasności w niniejszej umowie rozstrzyga się zgodnie z klauzulą 8.4.

8.4. **Prawo właściwe**

Niniejsza umowa podlega prawu (*określić państwo członkowskie*).

8.5. **Interpretacja**

8.5.1. Strony zawierają niniejszą umowę w kontekście praw i obowiązków stron wynikających z aktu w sprawie danych. Każde postanowienie niniejszej umowy należy interpretować w sposób zapewniający zgodność z aktem w sprawie danych oraz innymi przepisami prawa Unii lub przepisami krajowymi przyjętymi zgodnie z prawem Unii, a także z wszelkimi mającymi zastosowanie przepisami prawa krajowego, które są zgodne z prawem Unii i których nie można wyłączyć w drodze umowy.

8.5.2. Jeżeli jakiejkolwiek luki lub niejasności w niniejszej umowie nie można usunąć w sposób, o którym mowa w klauzuli 8.5.1, umowę tę należy interpretować w świetle zasad wykładni przewidzianych w prawie właściwym (zob. klauzula 8.4).

8.6. **Rozstrzyganie sporów**

8.6.1. Strony uzgadniają, że dołożą wszelkich starań w celu polubownego rozstrzygania sporów i że przed wniesieniem sprawy do sądu przekażą spór do (*wstawić nazwę i dane kontaktowe konkretnego organu rozstrzygania sporów; w odniesieniu do sporów mieszczących się w zakresie jego jurysdykcji określonej w art. 10 ust. 1 aktu w sprawie danych może to być każdy organ rozstrzygania sporów w państwie członkowskim, który spełnia warunki określone w art. 10 aktu w sprawie danych*).

8.6.1. [WARIANT – jeżeli użytkownik jest przedsiębiorstwem] [Sądy (*określić państwo członkowskie*) będą miały wyłączną właściwość do rozpoznania sprawy dotyczącej niniejszej umowy.]

Dodatek 1 zawiera opis danych

[do opracowania przez strony]

Dodatek 2 zawiera wykaz środków ochrony stosowanych przez odbiorcę danych

[do opracowania przez strony]

Dodatek 3 zawiera informacje na temat dzielenia się danymi z osobami trzecimi przez odbiorcę danych

[do opracowania przez strony]

Dodatek 4 zawiera informacje o rekompensacie dla użytkownika za wykorzystywanie danych i dzielenie się danymi przez odbiorcę danych

[do opracowania przez strony]

Dodatek 5 zawiera dokumentację dotyczącą własności produktu lub praw umownych do korzystania z produktu lub usług powiązanych

[do opracowania przez strony]

[WARIANT] Dodatek 6 zawiera szczegółowe informacje na temat kar

[do opracowania przez strony]

ZAŁĄCZNIK IV

MODELOWE POSTANOWIENIA UMOWNE

na potrzeby umów między posiadaczami danych a odbiorcami danych o udostępnianie danych na wniosek użytkowników produktów skomunikowanych i usług powiązanych

Poniższe modelowe postanowienia umowne opracowano na potrzeby umów między posiadaczem danych a odbiorcą danych będącym przedsiębiorstwem, w przypadkach gdy posiadacz danych jest zobowiązany (na podstawie art. 5 rozporządzenia (UE) 2023/2854 – zwanego dalej „aktem w sprawie danych") do udostępniania danych z produktu skomunikowanego lub usługi powiązanej odbiorcy danych na wniosek użytkownika.

Główną nowością wprowadzoną przez akt w sprawie danych w tym zakresie jest to, że:

— posiadacz danych jest zobowiązany do dzielenia się danymi z odbiorcą danych po otrzymaniu od użytkownika wniosku w tym zakresie (z zastosowaniem środków ochrony danych chronionych jako tajemnice przedsiębiorstwa);

— posiadacz danych może żądać od odbiorcy danych zasadnej rekompensaty;

— nieuczciwe postanowienia umowne dotyczące dostępu do danych i ich wykorzystywania lub odpowiedzialności i środków ochrony prawnej wobec naruszenia lub odstąpienia od obowiązków dotyczących danych nie są wiążące, jeżeli zostały nałożone na przedsiębiorstwo jednostronnie przez inne przedsiębiorstwo.

Umowa ma strukturę modułową i chociaż może być stosowana jako pełna umowa, strony mogą również wybrać niektóre klauzule odpowiadające ich konkretnej sytuacji. Kilka klauzul zawiera różne warianty, w związku z czym strony powinny przeanalizować swoje szczególne potrzeby, relacje biznesowe i interesy, aby wybrać wariant najlepiej pasujący do ich umowy.

Niektóre klauzule są również opatrzone komentarzem *(w stosownych przypadkach)* i powinny zostać włączone do umowy, jeżeli spełnione są określone warunki.

Chociaż modelowe postanowienia umowne są zalecane przez Komisję, nie są one wiążące i strony mogą od nich zawsze odstąpić.
Modelowe postanowienia umowne można również stosować po wprowadzeniu odpowiednich zmian, w przypadkach gdy posiadacz danych jest zobowiązany do udostępnienia danych odbiorcy danych na podstawie innych przepisów prawa Unii lub przepisów krajowych przyjętych zgodnie z prawem Unii.

1. Strony, wnioskujący użytkownik oraz produkt/usługi powiązane

1.1. Strony umowy

Niniejsza umowa o dostępie do danych i ich wykorzystywaniu zostaje zawarta

między

(*wstawić nazwę, dane kontaktowe i dalsze odniesienia*) („posiadacz danych")

a

(*wstawić nazwę, dane kontaktowe i dalsze odniesienia*) („odbiorca danych")

zwanymi w niniejszej umowie łącznie „stronami", a każdy indywidualnie „stroną".

W tym miejscu strony muszą określić, kto jest posiadaczem danych oraz kto jest odbiorcą danych w rozumieniu art. 2 pkt 13 i 14 aktu w sprawie danych.

Zgodnie z aktem w sprawie danych „posiadacz danych" oznacza osobę fizyczną lub prawną, która ma prawo lub obowiązek – zgodnie z aktem w sprawie danych, mającym zastosowanie prawem Unii lub prawem krajowym przyjętym zgodnie z prawem Unii – wykorzystywać i udostępniać dane, w tym, o ile zostało to przewidziane umową, dane z produktu lub dane z usługi powiązanej pobrane lub wygenerowane przez nią podczas świadczenia powiązanej usługi.

Zgodnie z aktem w sprawie danych „odbiorca danych" oznacza osobę fizyczną lub prawną działającą w celach związanych z jej działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, inną niż użytkownik produktu skomunikowanego lub usługi powiązanej, której to osobie posiadacz danych udostępnia dane, w tym osobę trzecią, na wniosek użytkownika skierowany do posiadacza danych lub zgodnie z obowiązkiem prawnym wynikającym z prawa Unii lub prawa krajowego przyjętego zgodnie z prawem Unii. Zgodnie z art. 1 ust. 3 lit. d) aktu w sprawie danych posiadacze danych są zobowiązani do udostępniania danych wyłącznie „odbiorcom danych w Unii". Nie są do tego zobowiązani w przypadku, gdy miejsce prowadzenia działalności odbiorcy danych znajduje się poza Unią.

1.2. **Wnioskujący użytkownik, produkt/usługi powiązane**

1.2.1. Niniejsza umowa opiera się na wspólnym założeniu stron, że posiadacz danych jest zobowiązany na mocy art. 5 aktu w sprawie danych do udostępnienia danych odbiorcy danych na wniosek złożony przez lub w imieniu

(*wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia*) („wnioskujący użytkownik")

oraz że wnioskujący użytkownik jest użytkownikiem (w rozumieniu art. 2 pkt 12 aktu w sprawie danych):

następującego produktu: (*wstawić nazwę i dalsze specyfikacje konkretnego produktu skomunikowanego lub rodzaju produktów objętych umową*) lub

następujących usług powiązanych: (*w stosownych przypadkach wstawić nazwę oraz dalsze specyfikacje konkretnych usług powiązanych użytkownika lub rodzaju usług powiązanych użytkownika objętych umową*).

W tym miejscu strony muszą określić, kto jest użytkownikiem w rozumieniu art. 2 pkt 12 aktu w sprawie danych, który występuje z wnioskiem do posiadacza danych na podstawie art. 5 aktu w sprawie danych.

„**Użytkownik**" oznacza osobę fizyczną lub prawną, która jest właścicielem produktu skomunikowanego lub której na podstawie umowy przekazane zostały tymczasowe prawa do korzystania z tego produktu skomunikowanego, lub która korzysta z usług powiązanych.

Strony muszą również określić, z którego produktu skomunikowanego oraz, w stosownych przypadkach, z której usługi powiązanej korzysta wnioskujący użytkownik.

Zgodnie z aktem w sprawie danych „**produkt skomunikowany**" oznacza rzecz:
(i) która pozyskuje, generuje lub zbiera dostępne dane dotyczące jej wykorzystywania lub jej otoczenia;
(ii) która jest w stanie komunikować dane z produktu za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu;
(iii) której podstawową funkcją nie jest przechowywanie, przetwarzanie ani przesyłanie danych w imieniu strony trzeciej, innej niż użytkownik.

„**Usługa powiązana**" oznacza usługę cyfrową (w tym oprogramowanie, ale z wyłączeniem usług łączności elektronicznej), która:
(i) podczas zakupu, najmu, dzierżawy lub leasingu jest skomunikowana z produktem w taki sposób, że jej brak uniemożliwiłby produktowi skomunikowanemu wykonywanie co najmniej jednej z jego funkcji lub
(ii) zostaje skomunikowana z produktem przez producenta lub osobę trzecią później, aby dodać, uaktualnić lub zmodyfikować funkcje produktu skomunikowanego.

2. **Podstawa umowy**

2.1. **Status wnioskującego użytkownika oraz istnienie ważnego wniosku**

2.1.1. Każda ze stron oświadcza, że według jej najlepszej wiedzy wnioskujący użytkownik jest użytkownikiem (w rozumieniu art. 2 pkt 12 aktu w sprawie danych) produktu i usług powiązanych określonych w klauzuli 1.2.1.

2.1.2. Każda ze stron oświadcza, że wnioskujący użytkownik zwrócił się do posiadacza danych z wnioskiem o udostępnienie odbiorcy danych danych określonych w klauzuli 3.1. Dowód złożenia wniosku załączono w **dodatku 1** do niniejszej umowy.

2.1.3. (*w stosownych przypadkach*) Każda ze stron oświadcza, że zgodnie z jej najlepszą wiedzą strona działająca w imieniu wnioskującego użytkownika otrzymała od wnioskującego użytkownika upoważnienie niezbędne do złożenia tego wniosku zgodnie z mającym zastosowanie prawem. Dowód upoważnienia załączono w **dodatku 1** do niniejszej umowy.

Zgodnie z aktem w sprawie danych wniosek może złożyć osoba trzecia działająca w imieniu wnioskującego użytkownika. Osobą trzecią może być na przykład osoba pośrednicząca w obrocie danymi lub inny agent bądź przedstawiciel, w tym również sam odbiorca danych.

Oczywiste jest, że w sytuacji, w której osoba trzecia – w tym odbiorca danych – twierdzi, iż została upoważniona przez wnioskującego użytkownika, taka sytuacja stanowi potencjalne źródło nadużyć w porównaniu ze standardowym przypadkiem złożenia wniosku bezpośrednio przez wnioskującego użytkownika. W związku z tym strony muszą podjąć zasadne kroki w celu sprawdzenia, czy nie doszło do oszustwa lub manipulacji oraz czy wniosek został prawidłowo złożony.

2.1.4. Każda ze stron oświadcza, że zgodnie z jej najlepszą wiedzą wniosek jest ważny na mocy mającego zastosowanie prawa, nie został wycofany ani nie utracił ważności.

Jeżeli istnieją przesłanki wskazujące, że wniosek jest nieważny lub został wycofany, strony muszą podjąć zasadne kroki w celu sprawdzenia, czy nadal istnieje wniosek, który jest ważny. W przeciwnym razie posiadacz danych może nie być uprawniony do dzielenia się danymi z odbiorcą danych i może ponosić za to odpowiedzialność. Odbiorca danych może również ponosić odpowiedzialność za wnioskowanie o dane, o które nie jest uprawniony wnioskować.

Ważność wniosku może zależeć od wielu czynników wynikających z mającego zastosowanie prawa. Na przykład, aby wniosek był prawnie wiążący, może być konieczne, aby:

— kwalifikował się jako dobrowolne, wystarczająco świadome i jednoznaczne oświadczenie woli wnioskującego użytkownika;

— został złożony przez osobę posiadającą wymaganą zdolność prawną i zdolność do czynności prawnych.

2.2. **Kwalifikowalność odbiorcy danych**

2.2.1. Odbiorca danych oświadcza, że między nim a wnioskującym użytkownikiem obowiązuje umowa, na podstawie której odbiorca danych jest uprawniony do wykorzystywania danych, oraz że zgodnie z tą umową będzie wykorzystywał dane wyłącznie do następujących celów (*wstawić cele zgodnie z umową między odbiorcą danych a wnioskującym użytkownikiem*):

(*jeżeli dane mogą ujawniać tajemnice przedsiębiorstwa*) Odbiorca danych oświadcza, że dane te są absolutnie niezbędne do osiągnięcia tego celu.

Zgodnie z art. 6 ust. 1 aktu w sprawie danych odbiorca danych może wykorzystywać dane wyłącznie na podstawie umowy zawartej z użytkownikiem oraz wyłącznie do celów uzgodnionych z użytkownikiem. W tym miejscu odbiorca danych powinien złożyć oświadczenia potwierdzające spełnienie powyższych warunków. Jeżeli oświadczenia te nie są prawdziwe lub przestaną być prawdziwe, posiadacz danych może mieć możliwość rozwiązania umowy zgodnie z klauzulą 2.4.3.

Strony powinny dążyć do ustalenia uzgodnionych celów w taki sposób, aby umożliwić posiadaczowi danych ocenę, czy wykorzystywanie danych przez odbiorcę danych jest dopuszczalne, jednak bez nadmiernej szczegółowości, w wyniku której odbiorcy danych mogłyby zostać ujawnione poufne pomysły biznesowe posiadacza danych.

W przypadku gdy w grę wchodzą tajemnice przedsiębiorstwa posiadacza danych, należy ujawnić pełne cele, aby umożliwić posiadaczowi danych ocenę, czy przekazanie danych jest absolutnie niezbędne do osiągnięcia zadeklarowanego celu.

2.2.2. Odbiorca danych oświadcza, że nie został wskazany jako „strażnik dostępu” na podstawie art. 3 rozporządzenia (UE) 2022/1925 („akt o rynkach cyfrowych”).

2.3. **Zgodność z przepisami o ochronie danych**

2.3.1. W zakresie, w jakim dane kwalifikują się jako dane osobowe, każda ze stron oświadcza, że przestrzega przepisów rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, dyrektywy 2002/58/WE.

2.3.2. W szczególności, jeżeli wnioskujący użytkownik nie jest osobą, której dane dotyczą, posiadacz danych może udostępnić odbiorcy danych dane będące danymi osobowymi wyłącznie w zakresie dozwolonym na mocy rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, dyrektywy 2002/58/WE.

Pojęcie „danych osobowych” w rozumieniu RODO ma bardzo szeroki zakres. Obejmuje ono wszelkie dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, tj. osoby fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość tej osoby fizycznej.

Dane nieosobowe mogą stać się danymi osobowymi, na przykład gdy stanowią część mieszanego zbioru danych, w którym są połączone z nowymi danymi, a efekt tego połączenia umożliwia powiązanie danych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Może to również mieć miejsce w przypadku pojawienia się nowych zdolności w zakresie przetwarzania danych.

Strony powinny zacząć od starannej oceny tego, czy dane obejmują dane osobowe, a także oceny ról swoich i użytkownika, na gruncie RODO:

— „osoba, której dane dotyczą” oznacza zidentyfikowaną lub możliwą do zidentyfikowania osobę fizyczną, której dotyczą informacje;

— „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; w przypadkach gdy cele i sposoby takiego przetwarzania są określone w przepisach prawa, to samo prawo może określać, kto jest administratorem;

— „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

— „odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (z wyłączeniem organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania prowadzonego na podstawie prawa właściwego).

Strony powinny wziąć pod uwagę, że strona może pełnić więcej niż jedną rolę w zależności od celu przetwarzania lub może pełnić jedną rolę wspólnie z inną stroną.

Do dzielenia się danymi z odbiorcą danych niezbędna jest podstawa prawna na mocy RODO. Podstawą prawną dzielenia się danymi osobowymi w przypadku, gdy wnioskujący użytkownik nie jest osobą, której dane dotyczą, może być na przykład zgoda osób, których dane dotyczą, w rozumieniu art. 6 ust. 1 lit. a) lub prawnie uzasadniony interes w rozumieniu art. 6 ust. 1 lit. f) RODO. Aby ocenić istnienie takiego prawnie uzasadnionego interesu, można wziąć pod uwagę obowiązek udostępnienia danych zgodnie z art. 5 aktu w sprawie danych, przy czym sam ten obowiązek nie stanowi wystarczającej podstawy prawnej.

2.4. **Nieprawidłowość oświadczeń**

2.4.1. Każda strona, która dowie się, że którekolwiek z oświadczeń, o których mowa w klauzulach od 2.1 do 2.3, nie jest lub przestało być prawidłowe lub przestanie być prawidłowe w dającej się przewidzieć przyszłości, musi bez zbędnej zwłoki powiadomić o tym drugą stronę, chyba że druga strona jest lub powinna być już świadoma tego faktu.

Jeżeli którekolwiek z oświadczeń, o których mowa w klauzulach od 2.1 do 2.3, nie jest lub przestało być prawidłowe, strona powinna podjąć odpowiednie kroki. W szczególności, jeżeli wnioskujący użytkownik sprzedał produkt i przestał być użytkownikiem, a posiadacz danych otrzymał stosowną informację, posiadacz danych powinien rozwiązać umowę z odbiorcą danych w odniesieniu do takiego użytkownika. W wypowiedzeniu należy wskazać przyczynę wypowiedzenia umowy. Samo przekazanie zawiadomienia nie byłoby w takim przypadku wystarczające, ponieważ nie istnieje możliwość zaradzenia tej sytuacji. Jeżeli odbiorca danych chce nadal otrzymywać dane, musi zwrócić się do nowego użytkownika. W niektórych przypadkach strony mogą jednak naprawić naruszenie dotyczące reprezentacji. Dotyczy to na przykład sytuacji, w której wniosek użytkownika został złożony przez osobę nieupoważnioną (np. pracownika, który nie był umocowany do reprezentowania przedsiębiorstwa użytkownika). W takim przypadku prawo właściwe może umożliwiać potwierdzenie takiej czynności z mocą wsteczną.

2.4.2. Po powzięciu wiadomości o takiej sytuacji dana strona musi podjąć odpowiednie działania i – w miarę możliwości – skorygować nieprawidłowość oświadczenia. W zależności od okoliczności może to obejmować zawiadomienie wnioskującego użytkownika lub każdej chronionej osoby trzeciej, której to dotyczy, lub tymczasowe zawieszenie udostępniania danych przez posiadacza danych lub wykorzystywania danych przez odbiorcę danych, jeżeli udostępnianie danych lub ich wykorzystywanie stało się niezgodne z prawem.

2.4.3. Jeżeli sytuacja nie zostanie naprawiona i nie może zostać naprawiona, niniejsza umowa musi zostać rozwiązana w drodze pisemnego wypowiedzenia przekazanego przez jedną ze stron drugiej stronie, zawierającego przyczyny rozwiązania umowy.

Rozwiązanie umowy następuje ze skutkiem natychmiastowym. W przypadku gdy nieprawidłowość dotyczy jedynie części danych objętych niniejszą umową, rozwiązanie wywołuje skutki wyłącznie w odniesieniu do tej części.

Skutki rozwiązania umowy reguluje klauzula 7.3.

3. **Udostępnianie danych**

3.1. **Dane objęte umową**

3.1.1. Dane objęte niniejszą umową obejmują łatwo dostępne dane z produktu lub usług powiązanych, w rozumieniu aktu w sprawie danych, wskazane we wniosku złożonym przez wnioskującego użytkownika zgodnie z art. 5 aktu w sprawie danych, i obejmują zarówno dane nieosobowe, jak i dane osobowe („dane”).

Dane te wymieniono szczegółowo w **dodatku 2**.

Jeżeli w trakcie obowiązywania niniejszej umowy konieczne będzie udostępnienie odbiorcy danych innych niż wymienione w **dodatku 2**, **dodatek 2** zostanie odpowiednio zmieniony.

W dodatku 2 strony powinny określić dane i metadane objęte umową, zgodnie z wnioskiem złożonym przez wnioskującego użytkownika.

Zgodnie z art. 5 i art. 2 pkt 15, 16 i 17 aktu w sprawie danych dane te mogą stanowić wyłącznie łatwo dostępne dane z produktu lub usługi powiązanej:

— dane z produktu to dane wygenerowane w wyniku korzystania z produktu skomunikowanego, które producent zaprojektował tak, by użytkownik, posiadacz danych lub osoba trzecia, w tym w stosownym przypadku producent, mogli je pobierać za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu;

— dane z usługi powiązanej to dane stanowiące cyfrowe odwzorowanie czynności lub zdarzeń z udziałem użytkownika związanych z produktem skomunikowanym, utrwalane przez użytkownika celowo lub generowane jako produkt uboczny jego czynności, podczas świadczenia usługi powiązanej;

— dane łatwo dostępne to dane, które posiadacz danych może zgodnie z prawem pozyskać z produktu lub z usługi powiązanej bez nieproporcjonalnie dużego wysiłku wykraczającego poza prostą czynność.

Ponieważ niniejsza umowa określa zasady udostępniania danych odbiorcy danych na wniosek złożony przez wnioskującego użytkownika, dane te stanowią dane wskazane w tym wniosku.

Opis danych musi być wystarczający do ustalenia, które dane są objęte szczegółowymi uregulowaniami – o ile takie występują. W szczególności strony powinny przedstawić szczegółowe informacje dotyczące tego, które dane kwalifikują się jako dane osobowe.

3.2. **Charakterystyka danych i ustalenia dotyczące dostępu**

3.2.1. Posiadacz danych jest obowiązany udostępnić dane odbiorcy danych, przy czym dane te muszą cechować się co najmniej taką samą jakością jak w chwili, gdy stały się dostępne dla posiadacza danych, i w każdym wypadku muszą być udostępnione w całościowym, ustrukturyzowanym, powszechnie używanym i nadającym się do odczytu maszynowego formacie, wraz z odpowiednimi metadanymi niezbędnymi do interpretacji i wykorzystania tych danych.

„Metadane” oznaczają ustrukturyzowany opis treści danych lub sposobu wykorzystywania danych, który ułatwia wyszukiwanie lub wykorzystywanie tych danych. Zgodnie z art. 5 ust. 1 aktu w sprawie danych metadane należy udostępniać wraz z danymi w zakresie, w jakim metadane są „niezbędne do interpretacji i wykorzystania” tych danych.

Chociaż nie określono odpowiednich metadanych potrzebnych do interpretacji i wykorzystania tych danych i w związku z tym trzeba je identyfikować indywidualnie dla każdego przypadku, w akcie w sprawie danych określono, że „[d]ane, które mają być udostępnione, powinny obejmować stosowne metadane, w tym ich podstawowy kontekst i znacznik czasu, aby dane były użyteczne w połączeniu z innymi danymi, takimi jak dane posortowane i sklasyfikowane z innymi odnoszącymi się do nich punktami danych, lub przeformatowane na powszechnie używany format" (motyw 15 aktu w sprawie danych).

3.2.2. Odbiorcy danych należy udzielić dostępu do danych:

a) w sposób łatwy i bezpieczny,

b) bez zbędnej zwłoki,

(*w stosownych przypadkach*) c) w sposób ciągły i w czasie rzeczywistym.

3.2.3. W celu spełnienia wymogów klauzul 3.2.1 i 3.2.2 strony uzgadniają specyfikacje określone w dodatku 2.

Zgodnie z art. 5 ust. 1 aktu w sprawie danych dane należy udostępniać bez zbędnej zwłoki oraz, w stosownych przypadkach i jeżeli jest to technicznie wykonalne, w sposób ciągły i w czasie rzeczywistym.

Ponieważ istnieją różne sposoby realizacji tych wymogów prawnych, strony powinny uzgodnić w **dodatku 2** wszystkie szczegółowe informacje dotyczące sposobu udzielania dostępu.

Powinny przy tym w pierwszej kolejności zdecydować, czy chcą przewidzieć:

— **pełne przekazanie** danych, tj. przekazanie kopii danych na nośnik pozostający pod kontrolą odbiorcy danych:

  — w drodze transmisji inicjowanej przez posiadacza danych („push"), takiej jak transmisja online, przesłanie do przestrzeni w chmurze odbiorcy danych lub dostarczenie materialnego nośnika, na którym przechowywane są dane, lub

  — w drodze pobrania inicjowanego przez odbiorcę danych („pull"), na przykład przez udostępnienie API, dostępu do przestrzeni w chmurze posiadacza danych lub podobnych narzędzi umożliwiających odbiorcy danych dostęp do danych i ich wyodrębnienie, lub

— **dostęp do danych w miejscu ich przechowywania**, tj. dostęp do danych i ich przetwarzanie na nośniku pozostającym pod kontrolą posiadacza danych lub zaufanej osoby trzeciej, na przykład przez zalogowanie się odbiorcy danych do specjalnej przestrzeni na serwerach posiadacza danych lub zaufanej osoby trzeciej, z zastrzeżeniem, że dane nie są przekazywane na nośnik pozostający pod kontrolą odbiorcy danych, chyba że poczyniono szczególne ustalenia w tym względzie.

Pełne przekazanie danych zapewnia odbiorcy danych maksymalną swobodę, ale znacznie ogranicza zdolność posiadacza danych do zapobiegania nadużyciom.

Dostęp do danych w miejscu ich przechowywania zwiększa ryzyko, że zostaną ujawnione pomysły biznesowe odbiorcy danych, ale znacznie zwiększa zdolność posiadacza danych do zapobiegania nadużyciom.

Poza pełnym przekazaniem danych oraz dostępem do danych w miejscu ich przechowywania istnieją również inne rozwiązania techniczne, w tym dostęp na urządzeniu wnioskującego użytkownika.

Jeżeli strony zdecydują się na dostęp do danych w miejscu ich przechowywania, konieczne jest rozstrzygnięcie szeregu kwestii, w tym zapewnienie, aby pomysły biznesowe odbiorcy danych nie zostały ujawnione, oraz określenie, jakie dane odbiorca danych może pobrać i przekazać na nośnik pozostający pod jego kontrolą (np. dane wywnioskowane lub dane wywiedzione w wyniku czynności przetwarzania wykonywanych przez odbiorcę danych).

Ogólnie rzecz biorąc, warunki dostępu do danych w miejscu ich przechowywania nie mogą naruszać żadnych praw przyznanych wnioskującemu użytkownikowi ani odbiorcy danych na mocy aktu w sprawie danych lub innego mającego zastosowanie prawa.

Często preferowanym rozwiązaniem będzie dostęp do danych przechowywanych na nośniku kontrolowanym przez zaufaną osobę trzecią, a nie przechowywanych na nośniku kontrolowanym przez posiadacza danych. Dostęp do danych w miejscu ich przechowywania powinien co do zasady oznaczać dostęp zdalny, natomiast dostęp na miejscu powinien być ograniczony do sytuacji skrajnych, charakteryzujących się najwyższym stopniem wrażliwości.

Strony muszą również określić czas udzielenia dostępu do danych. Zgodnie z art. 5 ust. 1 aktu w sprawie danych dane należy udostępniać, na wniosek użytkownika, bez zbędnej zwłoki oraz, w stosownych przypadkach i jeżeli jest to technicznie wykonalne, w sposób ciągły i w czasie rzeczywistym.

Taki dostęp nie zawsze jest jednak potrzebny do osiągnięcia celów uzgodnionych w danym przypadku między odbiorcą danych a wnioskującym użytkownikiem. W związku z tym strony muszą uzgodnić kwestie dotyczące czasu udzielania dostępu do danych, takie jak to, czy – w stosownych przypadkach i gdy jest to technicznie wykonalne – dostęp jest udzielany w czasie rzeczywistym, a jeżeli nie, to z jaką częstotliwością.

Strony muszą również rozważyć szereg innych kwestii, takich jak to, jakie dane uwierzytelniające są wymagane, oraz którzy pracownicy odbiorcy danych mogą uzyskać dostęp do danych – i ilu z nich.

3.2.4. Jeżeli dane są udostępniane zgodnie ze specyfikacjami zawartymi w dodatku dotyczącym charakterystyki danych i ustaleń dotyczących dostępu oraz jeżeli okaże się, że uzgodnione specyfikacje są niewystarczające do spełnienia wymogów, o których mowa w klauzulach 3.2.1 i 3.2.2, strony zobowiązują się do rozpoczęcia negocjacji w dobrej wierze i dostosowania specyfikacji w taki sposób, aby spełniały one uzgodnione wymogi.

3.2.5. Posiadacz danych jest obowiązany przekazać odbiorcy danych informacje niezbędne do uzyskania dostępu do danych lub ich otrzymania zgodnie z art. 5 aktu w sprawie danych.

Obejmuje to w szczególności przekazanie łatwo dostępnych posiadaczowi danych informacji dotyczących pochodzenia danych oraz wszelkich praw, jakie mogą przysługiwać osobom trzecim w odniesieniu do tych danych, takich jak prawa osób, których dane dotyczą, wynikające z rozporządzenia (UE) 2016/679 (RODO), lub okoliczności faktycznych, które mogą prowadzić do powstania takich praw.

Posiadacz danych określa te informacje w **dodatku 2**.

Strony zachowują swobodę uzgadniania wszelkiego dodatkowego wsparcia, wykraczającego poza wymogi aktu w sprawie danych, nieodpłatnie lub za opłatą.

3.2.6. Posiadacz danych zobowiązuje się nie przechowywać żadnych informacji na temat dostępu odbiorcy danych do danych, których dotyczy wniosek, poza informacjami, które są niezbędne do:

a) należytego wykonania (i) wniosku złożonego przez wnioskującego użytkownika o dostęp oraz (ii) niniejszej umowy,

b) zapewnienia bezpieczeństwa i utrzymania infrastruktury danych oraz

c) przestrzegania obowiązków prawnych posiadacza danych w zakresie przechowywania takich informacji.

3.3. **Mechanizm informacji zwrotnej**

3.3.1. Jeżeli odbiorca danych zidentyfikuje incydent związany z klauzulą 3.1 – dotyczącą danych objętych umową – lub klauzulą 3.2 – dotyczącą charakterystyki danych i ustaleń dotyczących dostępu – oraz jeżeli odbiorca danych przekaże posiadaczowi danych szczegółowy opis tego incydentu, posiadacz danych i odbiorca danych muszą współpracować w dobrej wierze w celu zidentyfikowania przyczyny incydentu. Jeżeli incydent został spowodowany niedopełnieniem obowiązków przez posiadacza danych, posiadacz danych jest zobowiązany usunąć naruszenie bez zbędnej zwłoki. Jeżeli posiadacz danych nie usunie naruszenia, uznaje się to za istotne naruszenie zobowiązania, a odbiorca danych ma prawo powołać się na klauzulę 8 niniejszej umowy (dotyczącą środków ochrony prawnej w przypadku naruszenia umowy).

3.3.2. Jeżeli osiągnięcie którejkolwiek ze specyfikacji uzgodnionych zgodnie z klauzulą 3.2 okaże się niemożliwe lub nadmiernie uciążliwe z powodu wyjątkowej zmiany okoliczności, która nastąpiła po zawarciu umowy, posiadacz danych musi przedstawić odbiorcy danych szczegółowy opis tej zmiany, a strony rozpoczną negocjacje w dobrej wierze i dostosują specyfikacje, tak aby spełniały one wymogi określone w niniejszych klauzulach. W szczególności każda ze stron musi przekazać drugiej stronie wystarczające informacje, aby umożliwić ocenę, omówienie i rozwiązanie danej sytuacji. Niniejsza klauzula nie narusza prawa odbiorcy danych do skorzystania ze środków ochrony prawnej zgodnie z klauzulą 8.

3.4. **Jednostronne zmiany dokonywane przez posiadacza danych**

3.4.1. Posiadacz danych może jednostronnie zmienić szczegóły specyfikacji charakterystyki danych i ustaleń dotyczących dostępu, jeżeli jest to obiektywnie uzasadnione zwykłym prowadzeniem działalności gospodarczej przez posiadacza danych, na przykład modyfikacją techniczną wynikającą z bezpośredniego zagrożenia bezpieczeństwa w odniesieniu do linii produktów lub usług powiązanych oferowanych przez posiadacza danych lub zmianą infrastruktury posiadacza danych. Każda zmiana musi spełniać wymogi klauzul 3.2.

3.4.2. Posiadacz danych musi zawiadomić odbiorcę danych o zmianie co najmniej (wskazać rozsądny okres) przed wejściem zmiany w życie.

Krótszy termin zawiadomienia może być wystarczający:

a) jeżeli zmiana nie ma negatywnego wpływu na dostęp do danych i ich wykorzystywanie przez odbiorcę danych lub

b) jeżeli takie zawiadomienie byłoby niemożliwe lub nierozsądne w danych okolicznościach, na przykład gdy natychmiastowe zmiany są wymagane ze względu na wykrycie bezpośredniego zagrożenia bezpieczeństwa.

3.4.3. W przypadku gdy zmiana negatywnie wpływa na dostęp do danych i ich wykorzystywanie przez odbiorcę danych, odbiorca danych jest uprawniony do rozwiązania (odpowiedniej części) umowy bez obowiązku zapłaty jakiejkolwiek rekompensaty na rzecz posiadacza danych, niezależnie od wszelkich innych praw lub środków ochrony prawnej przysługujących odbiorcy danych.

4. **(jeżeli dane muszą być chronione jako tajemnice przedsiębiorstwa) Ochrona tajemnic przedsiębiorstwa**

1. **Dzielenie się tajemnicami przedsiębiorstwa** – Posiadacze danych co do zasady nie mogą odrzucić wniosku o dostęp do danych wystosowanego na podstawie aktu w sprawie danych wyłącznie ze względu na to, że niektóre dane uznaje się za tajemnicę przedsiębiorstwa, ponieważ przeczyłoby to zamierzonym celom aktu w sprawie danych.

Zob. klauzule 4.1.

2. **Tajemnice przedsiębiorstwa** – Jeżeli jednak posiadacz danych stwierdzi, że niektóre dane objęte umową są chronione jako tajemnice przedsiębiorstwa w rozumieniu dyrektywy (UE) 2016/943[8] (zwanej dalej „dyrektywą w sprawie tajemnic przedsiębiorstwa"), przysługują mu określone prawa, w szczególności prawo do zachowania poufności informacji stanowiących tajemnicę przedsiębiorstwa.

Zgodnie z art. 2 pkt 1 dyrektywy w sprawie tajemnic przedsiębiorstwa termin „tajemnica przedsiębiorstwa" oznacza informacje, które spełniają trzy wymogi: a) są poufne w tym sensie, że jako całość lub w szczególnym zestawie i zbiorze ich elementów nie są ogólnie znane lub łatwo dostępne dla osób z kręgów, które zwykle zajmują się tym rodzajem informacji, b) mają wartość handlową dlatego, że są objęte tajemnicą, oraz c) poddane zostały przez osobę, która zgodnie z prawem sprawuje nad nimi kontrolę, rozsądnym, w danych okolicznościach, działaniom dla utrzymania ich w tajemnicy.

„Posiadacz tajemnicy przedsiębiorstwa" oznacza każdą osobę fizyczną lub prawną, która w sposób zgodny z prawem sprawuje kontrolę nad taką tajemnicą przedsiębiorstwa.

Dane można zidentyfikować jako tajemnice przedsiębiorstwa tylko wtedy, gdy są one chronione jako takie przez posiadacza danych lub posiadacza tajemnicy przedsiębiorstwa w przypadku złożenia wniosku o dostęp do danych zgodnie z art. 5 aktu w sprawie danych.

Zob. klauzula 4.1.1.

3. **Początkowa identyfikacja tajemnic przedsiębiorstwa** – Prawa posiadaczy danych w odniesieniu do tajemnic przedsiębiorstwa mają – początkowo – zastosowanie wyłącznie wtedy, gdy i wyłącznie w takim zakresie, w jakim dane chronione jako tajemnice przedsiębiorstwa zostały zidentyfikowane w umowie.

Zob. klauzula 4.1.2.

4. **W trakcie obowiązywania umowy** – Prawa posiadaczy danych w odniesieniu do tajemnic przedsiębiorstwa mogą jednak mieć również zastosowanie w trakcie obowiązywania umowy w odniesieniu do nowych danych, które mają zostać udostępnione na jej podstawie.

Zob. klauzula 4.1.3.

5. **Prawa do audytu** – W celu zachowania poufności danych chronionych jako tajemnice przedsiębiorstwa strony mogą rozważyć uwzględnienie pewnych praw do audytu realizowanych przez zaangażowanie niezależnych osób trzecich (nie ingerując w działania posiadacza danych ani odbiorcy danych), w tym mechanizmów na wypadek sporów dotyczących wyników zawartych w sprawozdaniu z audytu.

Zob. klauzula 4.2.3.

6. **Prawa posiadacza tajemnicy przedsiębiorstwa (1/4)** – Posiadacz danych (lub posiadacz tajemnicy przedsiębiorstwa będący osobą trzecią) może uzgodnić z odbiorcą danych wymogi dotyczące zachowania poufności tajemnic przedsiębiorstwa jako warunek udostępnienia tych zidentyfikowanych tajemnic przedsiębiorstwa, takie jak wprowadzenie określonych proporcjonalnych środków technicznych i organizacyjnych.

Zob. klauzule 4.2. i 4.3.

7. **Prawa posiadacza tajemnicy przedsiębiorstwa (2/4)** – Jeżeli początkowe środki okażą się niewystarczające, posiadacz tajemnicy przedsiębiorstwa może, w zależności od przypadku, w odniesieniu do konkretnych i zidentyfikowanych danych chronionych jako tajemnice przedsiębiorstwa, jednostronnie zwiększyć poziom stosowanych środków albo zwrócić się o uzgodnienie z odbiorcą danych dodatkowych środków. W przypadku braku porozumienia w sprawie niezbędnych środków posiadacz danych może zawiesić dzielenie się określonymi danymi chronionymi jako tajemnice przedsiębiorstwa na warunkach określonych w akcie w sprawie danych.

Zob. klauzula 4.4.2.

8. **Prawa posiadacza tajemnicy przedsiębiorstwa (3/4)** – Posiadacz tajemnicy przedsiębiorstwa może również, w zależności od przypadku, odmówić udostępnienia konkretnych, zidentyfikowanych tajemnic przedsiębiorstwa, jednak wyłącznie w wyjątkowych okolicznościach i na warunkach określonych w akcie w sprawie danych.

Zob. klauzula 4.4.3.

9. **Prawa posiadacza tajemnicy przedsiębiorstwa (4/4)** – Posiadacz tajemnicy przedsiębiorstwa może wstrzymać lub zawiesić dzielenie się danymi, jeżeli odbiorca danych narusza swoje obowiązki związane z ochroną tajemnic przedsiębiorstwa.

Zob. klauzula 4.4.4.

10. **Zatrzymywanie danych zawierających zidentyfikowane tajemnice przedsiębiorstwa** – Jeżeli posiadacz danych wstrzymuje lub zawiesza dzielenie się danymi zgodnie z klauzulami 4.4.1, 4.4.2 lub 4.4.3, posiadacz danych pozostaje zobowiązany do zapewnienia łatwego dostępu do powiązanych danych zawierających zidentyfikowane tajemnice przedsiębiorstwa przez ich zatrzymanie do czasu, gdy możliwe będzie ich udostępnienie w zakresie objętym umową.

Zob. klauzula 4.5.

11. **Posiadacz zidentyfikowanej tajemnicy przedsiębiorstwa będący osobą trzecią** – Jeżeli posiadacz tajemnicy przedsiębiorstwa jest osobą trzecią, posiadacz danych musi dopilnować, aby klauzula 4 chroniła również jego tajemnice przedsiębiorstwa, oraz uzyskać wszystkie odpowiednie upoważnienia od wspomnianego posiadacza tajemnicy przedsiębiorstwa będącego osobą trzecią.

Zob. klauzula 4.1.2.

4.1. **Stosowanie ustaleń dotyczących tajemnic przedsiębiorstwa**

4.1.1. Środki ochrony uzgodnione w klauzulach 4.2 i 4.3 niniejszej umowy, a także powiązane prawa uzgodnione w klauzulach 4.4 mają zastosowanie wyłącznie do danych lub metadanych zawartych w danych, które mają być udostępniane odbiorcy danych przez posiadacza danych i które są chronione jako tajemnice przedsiębiorstwa (zgodnie z definicją zawartą w art. 2 pkt 1 dyrektywy w sprawie tajemnic przedsiębiorstwa), będących w posiadaniu posiadacza danych lub innego posiadacza tajemnicy przedsiębiorstwa (zgodnie z definicją zawartą w art. 2 pkt 2 tej dyrektywy).

4.1.2. Identyfikację danych chronionych jako tajemnice przedsiębiorstwa oraz tożsamość posiadacza tajemnicy przedsiębiorstwa określono w dodatku 4.

Posiadacz danych oświadcza odbiorcy danych, że uzyskał wszystkie odpowiednie prawa od posiadaczy tajemnic przedsiębiorstwa będących osobami trzecimi do zawarcia niniejszej umowy w odniesieniu do danych chronionych jako tajemnice przedsiębiorstwa.

Zgodnie z art. 5 ust. 9 aktu w sprawie danych „[p]osiadacz danych lub, jeżeli nie jest to ta sama osoba, posiadacz tajemnicy przedsiębiorstwa identyfikują dane chronione, w tym stosowne metadane, jako tajemnice przedsiębiorstwa".
W związku z tym posiadacz danych powinien zidentyfikować dane chronione jako tajemnice przedsiębiorstwa w **dodatku 4**. Posiadacz danych nie powinien być jednak zobowiązany do opisania samej tajemnicy przedsiębiorstwa. Wystarczy, że zidentyfikuje dane, które muszą być chronione w celu zapewnienia poufności tajemnicy przedsiębiorstwa, ponieważ analiza takich danych mogłaby skutkować ujawnieniem tajemnicy przedsiębiorstwa.

4.1.3. Jeżeli w trakcie obowiązywania niniejszej umowy odbiorcy danych udostępnione zostaną nowe dane chronione jako tajemnice przedsiębiorstwa zgodnie z klauzulą 4.1.1, na wniosek posiadacza danych dodatek 4 zostanie odpowiednio zmieniony.

Do czasu zmiany i uzgodnienia przez strony treści dodatku 4 posiadacz danych może wstrzymać lub tymczasowo zawiesić dzielenie się danymi chronionymi jako tajemnice przedsiębiorstwa. W takim przypadku posiadacz danych należycie uzasadnia decyzję i bez zbędnej zwłoki przekazuje ją na piśmie użytkownikowi. Posiadacz danych zawiadamia również właściwy organ wyznaczony na podstawie art. 37 aktu w sprawie danych, że wstrzymał lub zawiesił dzielenie się danymi, oraz wskazuje, których środków nie uzgodniono ani nie wdrożono.

4.1.4. Zobowiązania określone w klauzulach 4.2 i 4.3 pozostają w mocy po każdym rozwiązaniu umowy, chyba że strony postanowią inaczej.

4.2. **Środki ochrony stosowane przez odbiorcę danych**

4.2.1. Odbiorca danych jest zobowiązany stosować środki ochrony określone w **dodatku 4** (zwane dalej „środkami ochrony leżącymi w gestii odbiorcy danych").

Strony powinny w odrębnym dodatku zawrzeć wszystkie szczegółowe informacje dotyczące tych środków, w tym sytuacji, gdy odbiorca danych dzieli się danymi z osobami trzecimi. Środki te mogą być zarówno techniczne (np. szyfrowanie, zapory sieciowe, przechowywanie danych w odrębnych lokalizacjach itp.), jak i organizacyjne (np. zarządzanie wewnętrzne, odpowiednie zarządzanie tożsamością i kontrole dostępu, zaangażowanie zaufanej osoby trzeciej).

Ponieważ środki muszą być proporcjonalne, ich treść będzie się różnić w zależności od charakteru tajemnicy przedsiębiorstwa. Środki te będą również zależały od tego, czy (i) udziela się dostępu do danych w miejscu ich przechowywania lub czy będzie to (ii) pełne przekazanie danych odbiorcy danych. W pierwszym przypadku posiadacz danych zachowuje wyższy stopień kontroli i może samodzielnie stosować część środków ochrony, podczas gdy odbiorca danych może mieć bardziej ograniczony zakres korzystania z danych. W każdym przypadku obie strony powinny koncentrować się na osiągnięciu zamierzonych skutków aktu w sprawie danych. Z tego względu konieczne jest wyważenie poszczególnych interesów, bez podważania tych zamierzonych skutków.

4.2.2. Jeżeli w niniejszej umowie i w umowie zawartej przez odbiorcę danych z użytkownikiem zezwolono odbiorcy danych na udostępnienie danych osobie trzeciej, odbiorca danych może dzielić się danymi chronionymi jako tajemnice przedsiębiorstwa, jeżeli:

a) bez zbędnej zwłoki poinformuje posiadacza danych o fakcie, że dane chronione jako tajemnice przedsiębiorstwa zostaną udostępnione osobie trzeciej, wskaże dane, których to dotyczy, oraz przekaże posiadaczowi danych informacje o tożsamości i miejscu prowadzenia działalności oraz dane kontaktowe osoby trzeciej.

b) osoba trzecia stosuje środki ochrony określone w dodatku 4.

4.2.3. [WARIANT] [W celu weryfikacji, czy i w jakim zakresie odbiorca danych wdrożył i utrzymuje środki ochrony leżące w gestii odbiorcy danych, odbiorca danych zgadza się (i) albo co roku uzyskiwać sprawozdanie z audytu oceny zgodności w zakresie bezpieczeństwa od niezależnej osoby trzeciej wybranej przez odbiorcę danych, albo (ii) co roku umożliwiać przeprowadzenie audytu oceny zgodności w zakresie bezpieczeństwa przez niezależną osobę trzecią wybraną przez posiadacza danych, pod warunkiem że taka niezależna osoba trzecia podpisała umowę o zachowanie poufności przedstawioną przez odbiorcę danych. Takie sprawozdanie z audytu bezpieczeństwa musi potwierdzać przestrzeganie przez odbiorcę danych klauzuli 4 oraz dodatku 4, w brzmieniu obowiązującym w danej chwili. Wyniki sprawozdań z audytu są przekazywane obu stronom bez zbędnej zwłoki.

Odbiorca danych może dokonać wyboru pomiędzy wariantem (i) a wariantem (ii). Jeżeli strona uzna sprawozdanie z audytu bezpieczeństwa za nieprawidłowe, zachowuje prawo do uzyskania sprawozdania z audytu bezpieczeństwa od innej niezależnej osoby trzeciej. W przypadku skorzystania z tego prawa obaj niezależni audytorzy będący osobami trzecimi, wraz ze stronami, omawiają wszelkie różnice między tymi dwoma sprawozdaniami i dążą do rozwiązania wszelkich nierozstrzygniętych kwestii, działając w dobrej wierze.]

Koszty takich sprawozdań z audytu ponoszone są w następujący sposób: (*określić zasady ponoszenia tych kosztów*).

Klauzula ta jest oznaczona jako wariant, ponieważ strony mogą uzgodnić inne środki służące weryfikacji, czy odbiorca danych wywiązuje się ze swoich zobowiązań w zakresie wdrażania i utrzymywania środków ochrony leżących w gestii odbiorcy danych.

4.3. **Środki ochrony stosowane przez posiadacza tajemnicy przedsiębiorstwa**

4.3.1. Posiadacz danych może stosować środki uzgodnione w **dodatku 4** w celu zachowania poufności danych chronionych jako tajemnice przedsiębiorstwa (zwane dalej „środkami ochrony stosowanymi przez posiadacza tajemnicy przedsiębiorstwa").

4.3.2. Posiadacz danych może również jednostronnie wdrożyć odpowiednie techniczne i organizacyjne rozwiązania ochronne, takie jak aktualizacje oprogramowania, jeżeli nie mają one negatywnego wpływu na odbiorcę danych w ramach niniejszej umowy.

4.3.3. Odbiorca danych zobowiązuje się nie zmieniać ani nie usuwać środków ochrony stosowanych przez posiadacza tajemnicy przedsiębiorstwa ani środków stosowanych zgodnie z klauzulą 4.3.2, chyba że strony postanowią inaczej.

4.4. **Obowiązek dzielenia się danymi i prawo do odmowy, wstrzymania lub rozwiązania umowy**

4.4.1. W przypadku gdy środki ochrony leżące w gestii odbiorcy danych oraz środki ochrony stosowane przez posiadacza tajemnicy przedsiębiorstwa nie są zasadniczo wystarczające do zapewnienia właściwej ochrony określonego elementu danych chronionych jako tajemnica przedsiębiorstwa, posiadacz danych może zwrócić się o uzgodnienie dodatkowych, niezbędnych środków technicznych lub organizacyjnych przez skierowanie do odbiorcy danych zawiadomienia zawierającego szczegółowy opis niewystarczalności tych środków. Jeżeli po upływie rozsądnego okresu nie zostanie osiągnięte porozumienie w sprawie takich środków i jeżeli potrzeba wprowadzenia takich środków zostanie należycie uzasadniona, np. w sprawozdaniu z audytu bezpieczeństwa, posiadacz danych może wstrzymać lub zawiesić dzielenie się konkretnymi danymi, których to dotyczy. W takim przypadku posiadacz danych musi zawiadomić odbiorcę danych i właściwy organ wyznaczony na podstawie art. 37 aktu w sprawie danych. Zawiadomienie to musi być należycie uzasadnione, wskazywać, które środki nie zostały uzgodnione oraz – w stosownych przypadkach – których tajemnic przedsiębiorstwa sprawa dotyczy, a także musi być przekazane na piśmie bez zbędnej zwłoki. Posiadacz danych jest obowiązany nadal dzielić się wszystkimi innymi danymi chronionymi jako tajemnica przedsiębiorstwa, z wyjątkiem tych konkretnych danych.

4.4.2. Jeżeli w wyjątkowych okolicznościach posiadacz danych jest w stanie wykazać, że istnieje duże prawdopodobieństwo, iż poniesie poważną szkodę ekonomiczną w wyniku ujawnienia odbiorcy danych określonych danych chronionych jako tajemnica przedsiębiorstwa pomimo wdrożenia środków ochrony leżących w gestii odbiorcy danych oraz, w stosownych przypadkach, środków ochrony stosowanych przez posiadacza tajemnicy przedsiębiorstwa, posiadacz danych może zawiesić dzielenie się tymi konkretnymi danymi.

Może to uczynić wyłącznie po przekazaniu odbiorcy danych oraz właściwemu organowi wyznaczonemu zgodnie z art. 37 aktu w sprawie danych należycie uzasadnionego zawiadomienia.

Posiadacz danych jest jednak obowiązany nadal dzielić się wszystkimi innymi danymi chronionymi jako tajemnica przedsiębiorstwa, z wyjątkiem tych konkretnych danych.

Odmowa lub zaprzestanie dzielenia się danymi na podstawie art. 5 aktu w sprawie danych są ograniczone do wyjątkowych okoliczności. W związku z tym zawiadomienie musi być należycie uzasadnione. Aspekty, które należy uwzględnić, mogą obejmować na przykład brak możliwości wyegzekwowania ochrony tajemnic przedsiębiorstwa w państwach niebędących członkami UE, charakter i poziom poufności danej tajemnicy przedsiębiorstwa lub niepowtarzalność i nowatorski charakter danego produktu skomunikowanego.

4.4.3. Jeżeli odbiorca danych nie wdroży i nie będzie utrzymywał środków ochrony leżących w gestii odbiorcy danych, a posiadacz danych należycie wykaże to uchybienie, na przykład w sprawozdaniu z audytu bezpieczeństwa, posiadacz danych jest uprawniony do wstrzymania lub zawieszenia dzielenia się konkretnymi zidentyfikowanymi tajemnicami przedsiębiorstwa do czasu, aż odbiorca danych zaradzi incydentowi.

W takim przypadku posiadacz danych musi bez zbędnej zwłoki przekazać odbiorcy danych oraz właściwemu organowi wyznaczonemu zgodnie z art. 37 aktu w sprawie danych należycie uzasadnione zawiadomienie na piśmie.

4.4.4. Klauzula 4.4.1 nie uprawnia posiadacza danych do rozwiązania umowy. Klauzule 4.4.2 lub 4.4.3 uprawniają posiadacza danych do rozwiązania umowy wyłącznie w odniesieniu do konkretnych zidentyfikowanych tajemnic przedsiębiorstwa oraz tylko wówczas, gdy:

a) wszystkie warunki określone w klauzulach 4.4.2 lub 4.4.3 zostały spełnione;

b) po upływie rozsądnego okresu strony nie osiągnęły porozumienia, pomimo podjęcia próby polubownego rozwiązania sporu, w tym po interwencji właściwego organu wyznaczonego na podstawie art. 37 aktu w sprawie danych, oraz

c) odbiorca danych nie uzyskał od właściwego sądu prawomocnego orzeczenia zobowiązującego posiadacza danych do udostępnienia danych ani nie toczy się żadne postępowanie sądowe w sprawie wydania takiego orzeczenia.

4.5. **Zatrzymywanie danych chronionych jako zidentyfikowane tajemnice przedsiębiorstwa**

4.5.1. W przypadku gdy posiadacz danych korzysta z prawa do wstrzymania lub zawieszenia dzielenia się danymi zgodnie z klauzulami 4.4.1, 4.4.2 oraz 4.4.3, musi zapewnić zatrzymywanie danych, tak aby dane te zostały udostępnione odbiorcy danych:

a) po uzgodnieniu i wdrożeniu odpowiednich środków ochrony lub

b) po wydaniu wiążącej decyzji przez właściwy organ lub sąd zobowiązującej posiadacza danych do przekazania danych odbiorcy danych.

Ten obowiązek zatrzymywania danych wygasa, gdy właściwy organ lub sąd w wiążącej decyzji zezwoli na usunięcie takich zatrzymywanych danych lub gdy umowa ulegnie rozwiązaniu zgodnie z klauzulą 4.4.4.

4.5.2. Posiadacz danych poniesie niezbędne koszty zatrzymywania danych na podstawie klauzuli 4.5.1. Odbiorca danych pokryje jednak takie koszty w zakresie, w jakim wstrzymanie lub zawieszenie dzielenia się danymi następuje zgodnie z klauzulą 4.4.3.

5. **Wykorzystywanie danych i dzielenie się danymi z osobami trzecimi**

5.1. **Dopuszczalne wykorzystywanie danych przez odbiorcę danych**

Odbiorca danych zobowiązuje się przetwarzać dane udostępnione mu na podstawie umowy wyłącznie do celów i na warunkach uzgodnionych z wnioskującym użytkownikiem.

Odbiorca danych musi usunąć dane, gdy nie są one już niezbędne do uzgodnionego celu, chyba że uzgodniono inaczej z wnioskującym użytkownikiem w odniesieniu do danych stanowiących dane nieosobowe.

5.2. **Dzielenie się danymi z osobami trzecimi**

5.2.1. Odbiorca danych nie może udostępniać danych innej osobie trzeciej, chyba że takie udostępnienie zostało uzgodnione umownie z wnioskującym użytkownikiem oraz jest zgodne z wszelkimi środkami ochrony uzgodnionymi z posiadaczem danych i z mającym zastosowanie prawem unijnym lub krajowym.

Odbiorca danych nie może w żadnym przypadku udostępniać otrzymanych danych przedsiębiorstwu wskazanemu jako strażnik dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925 (akt o rynkach cyfrowych).

5.2.2. W przypadku gdy odbiorca danych jest uprawniony do udostępnienia danych osobie trzeciej, musi wprowadzić odpowiednie środki umowne, techniczne i organizacyjne w celu zagwarantowania, że:

a) (*w stosownych przypadkach*) osoba trzecia stosuje co najmniej takie same środki ochrony, jakie odbiorca danych jest zobowiązany stosować na podstawie klauzuli 4.2, oraz respektuje środki ochrony stosowane przez posiadacza danych na podstawie klauzuli 4.3;

b) osoba trzecia wykorzystuje dane wyłącznie w sposób zgodny z klauzulami 5.1 i 5.3;

c) posiadaczowi danych przysługują wobec osoby trzeciej co najmniej takie same środki ochrony prawnej jak wobec odbiorcy danych w odniesieniu do wykorzystywania lub ujawniania danych zakazanych na mocy klauzuli 5.3.

5.2.3. Niezależnie od klauzul 5.2.1 i 5.2.2 odbiorca danych może – na własny rachunek i na własną odpowiedzialność – korzystać z usług przetwarzania danych, np. usług przetwarzania w chmurze (w tym infrastruktury jako usługi, platformy jako usługi i oprogramowania jako usługi), usług hostingu lub podobnych usług, w celu osiągnięcia uzgodnionych celów określonych w klauzuli 5.1. Osoby trzecie mogą również – na własny rachunek i na własną odpowiedzialność – korzystać z takich usług do celów, w jakich dane są im udostępniane.

5.3. **Nieuprawnione wykorzystywanie danych lub dzielenie się danymi**

5.3.1. Odbiorca danych nie może:

a) (do celów pozyskania danych) przekazywać posiadaczowi danych nieprawdziwych informacji, stosować środków wprowadzających w błąd lub środków przymusu ani wykorzystywać luk w infrastrukturze technicznej posiadacza danych mającej chronić dane; lub

b) nie dopełnić obowiązku utrzymywania umownych środków technicznych lub organizacyjnych uzgodnionych w klauzulach 4.2 i 4.3; lub

c) zmieniać ani usuwać, bez zgody posiadacza danych, technicznych środków ochrony stosowanych przez posiadacza danych w celu zapobiegania nieuprawnionemu dostępowi do danych oraz zapewnienia zgodności z niniejszą umową; lub

d) wykorzystywać otrzymanych danych w niedozwolonych celach, z naruszeniem klauzuli 5.1; lub

e) wykorzystywać danych do opracowania produktu konkurującego z produktem objętym niniejszą umową ani dzielić się w tym celu danymi z osobą trzecią;

f) wykorzystywać danych do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji posiadacza danych lub na temat wykorzystywania danych przez posiadacza danych;

g) wykorzystywać danych w sposób, który negatywnie wpływa na bezpieczeństwo produktu lub jakiejkolwiek usługi powiązanej;

h) wykorzystywać danych do profilowania osób fizycznych, chyba że jest to niezbędne do świadczenia usługi żądanej przez wnioskującego użytkownika;

i) ujawniać danych innej osobie trzeciej w sposób niezgodny z prawem lub z naruszeniem klauzul 5.2.1 i 5.2.2.

Jeżeli odbiorca danych dopuści się któregokolwiek z powyższych działań, stanowi to istotne naruszenie zobowiązania w rozumieniu klauzuli 8.1.1 i pociąga za sobą dodatkowe skutki określone w klauzuli 5.3.2.

5.3.2. W przypadkach, o których mowa w klauzuli 5.3.1, odbiorca danych musi bez zbędnej zwłoki zastosować się do żądań posiadacza danych lub wnioskującego użytkownika w zakresie:

a) poinformowania wnioskującego użytkownika o nieuprawnionym wykorzystaniu lub ujawnieniu danych oraz o środkach zastosowanych, aby położyć kres tej sytuacji;

b) usunięcia danych udostępnionych przez posiadacza danych na podstawie niniejszej umowy lub uzyskanych w sposób nieuprawniony lub stanowiący nadużycie, wraz z wszelkimi ich kopiami;

c) zapłaty rekompensaty na rzecz posiadacza danych, wnioskującego użytkownika lub innej chronionej osoby trzeciej za wszelką szkodę poniesioną w wyniku nieuprawnionego wykorzystania lub ujawnienia danych oraz

d) zaprzestania produkcji, oferowania, wprowadzania do obrotu lub wykorzystywania towarów, danych wywnioskowanych lub usług wytworzonych na podstawie wiedzy pozyskanej dzięki takim danym lub przywozu, wywozu lub magazynowania do tych celów towarów naruszających prawo oraz

e) zniszczenia wszelkich towarów naruszających prawo, w przypadku gdy (i) istnieje poważne ryzyko, że niezgodne z prawem wykorzystywanie tych danych spowoduje znaczną szkodę dla posiadacza danych, posiadacza tajemnicy przedsiębiorstwa lub użytkownika, lub (ii) gdy taki środek nie byłby nieproporcjonalny w świetle interesów posiadacza danych, posiadacza tajemnicy przedsiębiorstwa lub użytkownika.

6. **Rekompensata za zapewnienie dostępu do danych**

Strony powinny określić szczegóły dotyczące rekompensaty w samej umowie lub w oddzielnym dodatku.

Powinny one uzgodnić co najmniej:

— kwotę należnej rekompensaty oraz walutę,

— termin, w którym płatność staje się wymagalna,

— uzgodnienia dotyczące płatności.

Zgodnie z aktem w sprawie danych taka rekompensata może zawsze obejmować rekompensatę kosztów poniesionych w związku z udostępnieniem danych. Może ona obejmować również marżę, z wyjątkiem sytuacji, gdy odbiorcą danych jest MŚP lub organizacja nienastawiona na zysk. W każdym przypadku wysokość rekompensaty musi być zasadna.

Zgodnie z art. 9 ust. 2 aktu w sprawie danych przy ustalaniu wysokości rekompensaty należy uwzględnić „koszty poniesione w celu udostępnienia danych, w tym w szczególności koszty niezbędne do sformatowania danych, rozpowszechnienia danych za pomocą środków elektronicznych i ich przechowywania", a także – jeżeli rekompensata obejmuje marżę – „inwestycje poczynione w zebranie i wytworzenie danych, w stosownym przypadku z uwzględnieniem, czy do pozyskania, wygenerowania lub zebrania przedmiotowych danych przyczyniły się inne strony".

Zgodnie z art. 9 ust. 3 aktu w sprawie danych rekompensata może również zależeć od ilości, formatu i charakteru danych. Zgodnie z art. 9 ust. 7 aktu w sprawie danych posiadacz danych musi w każdym przypadku przedstawić informacje określające podstawę obliczenia rekompensaty w sposób wystarczająco szczegółowy, aby odbiorca danych mógł ocenić, czy spełnione zostały wymogi prawne.

6.1. **(ma zastosowanie, jeżeli odbiorca danych kwalifikuje się jako MŚP/organizacja badawcza nienastawiona na zysk)**

6.1.1. Odbiorca danych oświadcza, że jest MŚP w rozumieniu zalecenia 2003/361/WE *lub* organizacją badawczą nienastawioną na zysk. Ponadto oświadcza, że nie posiada przedsiębiorstw partnerskich ani powiązanych („przedsiębiorstwa") w rozumieniu art. 3 załącznika do zalecenia 2003/361/WE, które nie kwalifikują się jako MŚP.

[WARIANT] [Dowody na potwierdzenie powyższego przedstawiono w **dodatku 3**.]

6.1.2. Strony uzgadniają, że odbiorca danych wypłaci posiadaczowi danych rekompensatę [WARIANT 1] [w następujący sposób: (*określić*)] [WARIANT 2] [jak określono w **dodatku 3**].

6.1.3. Posiadacz danych oświadcza, że uzgodniona rekompensata nie przekracza kosztów bezpośrednio związanych z udostępnieniem danych odbiorcy danych i przypisywalnych do danego wniosku. Koszty te obejmują koszty, które trzeba ponieść w związku ze zwielokrotnieniem danych, rozpowszechnieniem danych za pomocą środków elektronicznych i przechowywaniem danych, ale nie ze zbieraniem lub tworzeniem danych.

Informacje określające podstawę obliczania rekompensaty, umożliwiające odbiorcy danych sprawdzenie, czy wymogi te zostały spełnione, są przekazywane przez posiadacza danych w **dodatku 3**.

6.1.4. Odbiorca danych niezwłocznie poinformuje posiadacza danych o wszelkich zmianach, które podważają zakwalifikowanie go jako MŚP.

W przypadku gdy odbiorca danych przestaje kwalifikować się jako MŚP, strony zobowiązują się do rozpoczęcia negocjacji w sprawie kwoty zasadnej rekompensaty. Jeżeli po upływie rozsądnego okresu nie zostanie osiągnięte porozumienie, posiadacz danych może zawiesić dzielenie się danymi, zawiadamiając o tym odbiorcę danych.

W takim przypadku posiadacz danych musi zapewnić zatrzymywanie danych, tak aby dane te zostały udostępnione odbiorcy danych po uzgodnieniu rekompensaty lub po wydaniu wiążącej decyzji przez właściwy organ lub sąd zobowiązującej posiadacza danych do przekazania danych odbiorcy danych.

Posiadacz danych poniesie niezbędne koszty zatrzymywania danych. Odbiorca danych musi jednak zrekompensować posiadaczowi danych wszelkie szkody ekonomiczne poniesione przez posiadacza danych w związku z tym, że odbiorca danych go nie poinformował.

6.2. **(ma zastosowanie, jeżeli odbiorca danych nie kwalifikuje się jako MŚP/organizacja badawcza nienastawiona na zysk)**

6.2.1. Strony uzgadniają, że odbiorca danych wypłaci posiadaczowi danych rekompensatę [WARIANT 1] [w następujący sposób: (*określić*)] [WARIANT 2] [jak określono w **dodatku 3**].

Informacje określające podstawę obliczania rekompensaty, umożliwiające odbiorcy danych sprawdzenie, czy wymogi te zostały spełnione, są przekazywane przez posiadacza danych w **dodatku 3**.

6.2.2. (*ma zastosowanie w przypadku rekompensaty pieniężnej*) W przypadku opóźnienia w zapłacie rekompensaty odbiorca danych powinien zapłacić posiadaczowi danych odsetki od zaległej rekompensaty za okres od dnia, w którym płatność stała się wymagalna, do dnia jej dokonania, zgodnie z prawem właściwym.

6.2.3. Jeżeli odbiorca danych zacznie kwalifikować się jako MŚP i poinformuje o tym posiadacza danych, strony zobowiązują się do zmiany kwoty zasadnej rekompensaty zgodnie z art. 9 ust. 4 aktu w sprawie danych.

7. **Data rozpoczęcia stosowania, okres obowiązywania i rozwiązanie umowy**

7.1. **Data rozpoczęcia stosowania i okres obowiązywania**

7.1.1. Niniejsza umowa [WARIANT 1] [wchodzi w życie ze skutkiem natychmiastowym] [WARIANT 2] [wchodzi w życie z dniem (*wskazać datę*)].

7.1.2. [WARIANT] [Niniejsza umowa zostaje zawarta [WARIANT 1] [na czas nieokreślony] [WARIANT 2] [na czas określony (*wskazać*)], z zastrzeżeniem wszelkich podstaw do jej wygaśnięcia lub rozwiązania przewidzianych w niniejszej umowie.]

Przy ustalaniu okresu obowiązywania umowy strony powinny kierować się przede wszystkim wnioskiem użytkownika oraz umową zawartą między użytkownikiem a odbiorcą danych. Jeżeli wniosek dotyczy **jednorazowego dostarczenia danych**, wystarczy uzgodnić datę rozpoczęcia stosowania.

Jeżeli wniosek dotyczy **ciągłego dostarczania danych**, strony będą musiały uzgodnić okres obowiązywania umowy oraz wybrać umowę na czas nieokreślony albo umowę na czas określony, w zależności od tego, czy wnioskujący użytkownik wskazał konkretny okres.

7.1.3. [WARIANT] [Posiadacz danych musi rozpocząć udostępnianie danych odbiorcy danych [WARIANT 1] [bez zbędnej zwłoki po wejściu w życie umowy] [WARIANT 2] [w dniu (*wskazać datę oraz – w stosownych przypadkach – dalsze szczegóły dotyczące terminów*)].]

Zazwyczaj strony chcą, aby wykonywanie umowy rozpoczęło się natychmiast po jej wejściu w życie. Nie musi tak być jednak w każdym przypadku, na przykład gdy jedna ze stron musi lub obie strony muszą jeszcze przygotować się do rozpoczęcia wykonywania umowy.

7.2. **Rozwiązanie umowy**

7.2.1. Niezależnie od okresu obowiązywania umowy uzgodnionego w klauzuli 7.1.1 i bez uszczerbku dla klauzuli 2.4.3 niniejsza umowa ulega rozwiązaniu:

a) z chwilą zniszczenia produktu lub trwałego zaprzestania świadczenia usługi powiązanej lub gdy produkt lub usługa powiązana w sposób nieodwracalny utracą zdolność generowania danych lub

b) jeżeli obie strony tak postanowią.

7.2.2. Odbiorca danych może rozwiązać umowę w dowolnym momencie okresu obowiązywania umowy, przekazując posiadaczowi danych wypowiedzenie z zachowaniem okresu (*wskazać okres*). Odbiorca danych musi zawiadomić wnioskującego użytkownika o rozwiązaniu umowy.

[WARIANT] Jeżeli odbiorca danych rozwiąże umowę na podstawie niniejszej klauzuli przed (*wskazać moment w czasie lub minimalny okres obowiązywania umowy*), musi wypłacić posiadaczowi danych rekompensatę za koszty poniesione przez posiadacza danych w związku z udostępnieniem danych, w następujący sposób: (*określić*).

Mogą wystąpić przypadki, w których posiadacz danych ponosi wydatki na udostępnienie danych odbiorcy danych, takie jak dostosowanie swojej infrastruktury cyfrowej, przy założeniu, że wydatki te z czasem się zamortyzują.

W takim przypadku posiadacz danych może chcieć zapewnić sobie otrzymanie rekompensaty od odbiorcy danych.

7.3. **Skutki wygaśnięcia i rozwiązania umowy**

7.3.1. Wygaśnięcie okresu obowiązywania umowy lub rozwiązanie niniejszej umowy zwalnia obie strony z zobowiązania do wykonania oraz do przyjęcia przyszłego świadczenia, lecz nie wpływa na prawa i zobowiązania, które powstały do chwili wygaśnięcia lub rozwiązania umowy.

Wygaśnięcie lub rozwiązanie umowy nie ma wpływu na żadne postanowienie, które ma obowiązywać nawet po wygaśnięciu umowy, w szczególności na wszelkie ograniczenia dotyczące dopuszczalnego wykorzystywania danych i dzielenia się danymi przez odbiorcę danych na podstawie klauzuli 5, klauzuli 4 – dotyczącej tajemnic przedsiębiorstwa, klauzuli 9.1 – dotyczącej poufności, klauzuli 9.5 – dotyczącej prawa właściwego, oraz klauzuli 9.7 – dotyczącej rozstrzygania sporów.

7.3.2. [WARIANT 1] [Przy zakończeniu umowy posiadacz danych musi zastosować odpowiednie środki wsparcia odejścia, jakich odbiorca danych może zasadnie oczekiwać.] [WARIANT 2] [Przy zakończeniu umowy posiadacz danych musi zastosować następujące środki wsparcia odejścia:] (*określić*)]

Strony mogą rozważyć, czy odbiorca danych wymaga jakichkolwiek środków wsparcia odejścia przy zakończeniu umowy.

Będzie to miało znaczenie na przykład w przypadku, gdy odbiorca danych był uprawniony do wyodrębnienia danych z nośnika lub środowiska kontrolowanego przez posiadacza danych, lecz nie wyodrębnił jeszcze tych danych, ponieważ nie spodziewał się rozwiązania umowy.

8. **Środki ochrony prawnej w przypadku naruszenia umowy**

Strony mogą chcieć uzgodnić nie tylko prawa i obowiązki dotyczące danych (z których wiele wynika już z aktu w sprawie danych), ale również kwestie z zakresu ogólnego prawa zobowiązań, takie jak prawa i środki ochrony prawnej przysługujące stronie umowy w przypadku niewykonania zobowiązania przez drugą stronę umowy.

W odniesieniu do takich kwestii z zakresu ogólnego prawa zobowiązań strony mogą chcieć oprzeć się na ustawowych przepisach dyspozytywnych lub na innych wzorach umów.

Jeżeli chcą skorzystać z niniejszych modelowych postanowień umownych, powinny upewnić się, że są one zgodne z wszelkimi bezwzględnie obowiązującymi przepisami prawa krajowego, które mogą mieć zastosowanie do tej umowy.

8.1. **Przypadki niewykonania zobowiązania**

8.1.1. Niewykonanie zobowiązania przez stronę jest istotnym naruszeniem zobowiązania, jeżeli:

a) niewykonanie zobowiązania w znacznym stopniu pozbawia drugą stronę tego, czego miała prawo oczekiwać na podstawie niniejszej umowy, chyba że strona, która nie wykonała zobowiązania, nie przewidziała i nie mogła w rozsądny sposób przewidzieć takiego rezultatu, lub

b) z okoliczności jasno wynika, że nie można polegać na przyszłym wykonaniu zobowiązań przez stronę, która nie wykonała zobowiązania.

8.1.2. Niewykonanie zobowiązania przez stronę jest usprawiedliwione, jeżeli wynika z przeszkody pozostającej poza jej kontrolą oraz jeżeli nie można było w rozsądny sposób oczekiwać, aby w chwili zawarcia niniejszej umowy strona ta uwzględniła tę przeszkodę bądź jej uniknęła lub przezwyciężyła ją lub jej skutki.

Jeżeli przeszkoda jest tylko tymczasowa, niewykonanie zobowiązania przez stronę jest usprawiedliwione tylko w okresie, w którym istnieje przeszkoda. Jeżeli jednak opóźnienie stanowi istotne naruszenie zobowiązania, druga strona może je tak traktować.

Strona, która nie wykonała zobowiązania, ma obowiązek dopilnować, aby zawiadomienie o przeszkodzie oraz jej wpływie na możliwość wykonania zobowiązania dotarło do drugiej strony bez zbędnej zwłoki po tym, jak strona, która nie wykonała zobowiązania, dowiedziała się lub powinna była się dowiedzieć o tych okolicznościach. Druga strona jest uprawniona do odszkodowania za szkodę ekonomiczną wynikłą z nieotrzymania takiego zawiadomienia.

8.2. **Środki ochrony prawnej w przypadku niewykonania zobowiązania**

8.2.1. W przypadku niewykonania zobowiązania przez jedną ze stron drugiej stronie przysługują środki ochrony prawnej wymienione w poniższych klauzulach, bez uszczerbku dla wszelkich środków ochrony prawnej dostępnych na podstawie prawa właściwego.

8.2.2. Dopuszczalne jest łączenie środków ochrony prawnej, które wzajemnie się nie wykluczają.

8.2.3. Strona nie może skorzystać ze środka ochrony prawnej w zakresie, w jakim sama spowodowała niewykonanie zobowiązania przez drugą stronę, na przykład gdy uchybienie w jej własnej infrastrukturze danych uniemożliwiło drugiej stronie należyte wykonanie jej zobowiązań. Strona nie może również powoływać się na roszczenie odszkodowawcze z tytułu poniesionych szkód w zakresie, w jakim mogła ograniczyć powstałą szkodę przez podjęcie zasadnych kroków.

8.2.4. Strona poszkodowana może:

a) żądać, aby strona, która nie wykonała zobowiązania, bez zbędnej zwłoki wykonała swoje zobowiązania wynikające z niniejszej umowy, chyba że byłoby to niezgodne z prawem lub niemożliwe lub wykonanie zobowiązania powodowałoby dla strony, która nie wykonała zobowiązania, koszty niewspółmierne do korzyści, jakie uzyskałaby druga strona;

b) wstrzymać się z wykonaniem swojego zobowiązania na podstawie niniejszej umowy, chyba że można przewidzieć, że spowodowałoby to szkodę dla strony, która nie wykonała zobowiązania, wyraźnie nieproporcjonalną do wagi niewykonania zobowiązania (w stosownych przypadkach) [pod warunkiem że spełnione są wszystkie warunki określone w klauzuli 4.4.4, jeżeli odbiorca danych nie wdroży lub nie utrzyma środków ochrony leżących w gestii odbiorcy danych uzgodnionych w klauzuli 4.2.1];

c) rozwiązać niniejszą umowę ze skutkiem natychmiastowym i bez ponoszenia kar, w drodze wypowiedzenia złożonego drugiej stronie, jeżeli:

(i) niewykonanie zobowiązania przez drugą stronę stanowi istotne naruszenie zobowiązania lub

(ii) w przypadku niewykonania, które nie stanowi istotnego naruszenia zobowiązania, strona poszkodowana przekazała zawiadomienie wyznaczające rozsądny termin na usunięcie uchybienia, a termin ten upłynął bez wykonania zobowiązania przez drugą stronę;

(iii) (*w stosownych przypadkach*) [pod warunkiem że spełnione są wszystkie warunki określone w klauzuli 4.4.5 – w przypadkach opisanych w klauzulach 4.4.2 lub 4.4.3;]

d) dochodzić odszkodowania za szkodę ekonomiczną poniesioną w wyniku niewykonania zobowiązania przez drugą stronę, jeżeli to niewykonanie nie jest usprawiedliwione na mocy klauzuli 8.1.2. Strona, która nie wykonała zobowiązania, ponosi odpowiedzialność wyłącznie za szkodę, którą przewidywała lub którą mogła w rozsądny sposób przewidzieć w chwili zawarcia niniejszej umowy jako skutek niewykonania zobowiązania, chyba że niewykonanie zobowiązania miało charakter umyślny lub stanowiło rażące zaniedbanie.

8.2.5. [WARIANT] W przypadku gdy strona nie wykona swoich zobowiązań wynikających z niniejszej umowy, jest ona w każdym przypadku zobowiązana do zapłaty kar umownych określonych szczegółowo w **dodatku 5**, które strony uznają za odszkodowanie w rozumieniu klauzuli 8.2.4 lit. d). Stronie, która nie wykonała zobowiązania, przysługuje prawo żądania obniżenia kary do rozsądnej wysokości, jeżeli strona ta wykaże, że kara jest rażąco wygórowana w stosunku do szkody wynikającej z niewykonania zobowiązania.

Strony mogą chcieć ustalić kary za określone rodzaje niewykonania zobowiązania, ponieważ udowodnienie przez stronę poszkodowaną kwoty rzeczywistej szkody spowodowanej np. niedostarczeniem danych może być zbyt uciążliwe. Kary powinny być proporcjonalne.

9. Postanowienia ogólne

9.1. Poufność

9.1.1. Następujące informacje muszą być uważane za poufne:

a) informacje odnoszące się do tajemnic przedsiębiorstwa, sytuacji finansowej lub jakiegokolwiek innego aspektu działalności strony, chyba że dana strona sama podała te informacje do publicznej wiadomości;

b) informacje określające podstawę obliczenia zasadnej rekompensaty;

c) informacje dotyczące wnioskującego użytkownika i wszelkich osób trzecich, chyba że informacje te zostały już podane przez nich do wiadomości publicznej.

9.1.2. Obie strony zgadzają się zastosować wszelkie uzasadnione środki w celu bezpiecznego przechowywania informacji poufnych i nie udostępniać takich informacji osobom trzecim, chyba że:

a) jedna ze stron jest prawnie zobowiązana do udostępnienia odpowiednich informacji, np. w celu wypełnienia obowiązku przekazania informacji wykazujących, że nie doszło do dyskryminacji zgodnie z art. 8 ust. 3 aktu w sprawie danych, lub

b) jedna ze stron musi udostępnić odpowiednie informacje w celu wypełnienia swoich zobowiązań wynikających z niniejszej umowy, lub

c) jedna ze stron uzyskała uprzednią zgodę drugiej strony lub strony, która przekazała informacje poufne lub której ujawnienie tych informacji dotyczy.

9.1.3. W każdym przypadku posiadacz danych może ujawnić lub udostępnić [WARIANT 1] [umowę wnioskującemu użytkownikowi] [WARIANT 2] [wnioskującemu użytkownikowi takie informacje, jakie są niezbędne, aby posiadacz danych mógł wykazać wypełnienie swoich zobowiązań (i) wobec odbiorcy danych na podstawie art. 5 aktu w sprawie danych lub (ii) wynikających z umowy zawartej z wnioskującym użytkownikiem na podstawie art. 4 ust. 6 aktu w sprawie danych].

9.1.4. Te zobowiązania do zachowania poufności pozostają w mocy po rozwiązaniu niniejszej umowy przez okres (*wskazać okres*).

9.1.5. Te zobowiązania do zachowania poufności nie znoszą ani nie ograniczają bardziej rygorystycznych obowiązków wynikających z (i) RODO, (ii) przepisów wdrażających dyrektywę 2002/58/WE lub dyrektywę (UE) 2016/943 ani (iii) żadnego innego prawa Unii ani prawa państwa członkowskiego.

9.2. **Niedyskryminacja**

Posiadacz danych oświadcza, że postanowienia niniejszej umowy ani żadne praktyki związane z jej wykonywaniem nie prowadzą do dyskryminacji porównywalnych kategorii odbiorców danych, w tym żadnego z ich partnerów lub przedsiębiorstw powiązanych („przedsiębiorstwa"), zgodnie z definicją zawartą w art. 3 załącznika do zalecenia 2003/361/WE, przy udostępnianiu danych.

Jeżeli odbiorca danych uważa, że warunki, na których dane zostały mu udostępnione, są dyskryminujące, posiadacz danych musi bez zbędnej zwłoki przedstawić odbiorcy danych, na jego uzasadniony wniosek, informacje wykazujące, że nie doszło do dyskryminacji.

9.3. **Środki komunikacji**

Wszelkie zawiadomienia lub inne komunikaty wymagane na mocy niniejszej umowy muszą mieć formę pisemną i mogą być doręczane osobiście, wysyłane pocztą przesyłką opłaconą z góry lub przekazywane drogą elektroniczną, w tym pocztą elektroniczną, pod warunkiem że nadawca zachowa dowód wysłania na adresy wskazane poniżej:

Strona	Osoba wyznaczona do kontaktów	E-mail	Telefon	Adres
Użytkownik	[Imię i nazwisko]/[Stanowisko]	[E-mail]	[Telefon]	[Adres]
Odbiorca danych	[Imię i nazwisko]/[Stanowisko]	[E-mail]	[Telefon]	[Adres]

Każde takie zawiadomienie lub każdy taki komunikat uznaje się za otrzymane:

a) w przypadku doręczenia osobistego – w dniu doręczenia,

b) w przypadku wysłania pocztą przesyłką opłaconą z góry – w trzecim dniu roboczym po dniu nadania,

c) w przypadku przekazania drogą elektroniczną – w dniu przekazania, pod warunkiem że nadawca nie otrzymał żadnego komunikatu o błędzie wskazującego na niedoręczenie.

9.4. **Całość umowy, zmiany i rozdzielność postanowień**

9.4.1. Niniejsza umowa (wraz z **dodatkami**, o których mowa w niniejszej umowie) stanowi całość umowy między stronami w odniesieniu do jej przedmiotu i zastępuje wszelkie wcześniejsze umowy i uzgodnienia stron – zarówno ustne, jak i pisemne – dotyczące przedmiotu niniejszej umowy.

9.4.2. Wszelkie zmiany niniejszej umowy będą ważne wyłącznie wtedy, gdy zostaną uzgodnione przez strony na piśmie, w tym w jakiejkolwiek formie elektronicznej.

9.4.3. Jeżeli którekolwiek postanowienie niniejszej umowy zostanie uznane za nieważne, bezskuteczne, wzruszalne lub niewykonalne z jakiegokolwiek powodu i jeżeli postanowienie to można oddzielić od pozostałych postanowień umowy, te pozostałe postanowienia pozostaną ważne i wykonalne. Wszelkie powstałe w ten sposób luki lub niejasności w niniejszej umowie rozstrzyga się zgodnie z klauzulą 9.6.

9.5. **Prawo właściwe**

Niniejsza umowa musi podlegać prawu (określić państwo członkowskie).

9.6. **Interpretacja**

9.6.1. Strony zawierają niniejszą umowę w kontekście praw i obowiązków stron wynikających z aktu w sprawie danych. Każde postanowienie niniejszej umowy należy interpretować w sposób zapewniający zgodność z aktem w sprawie danych oraz innymi przepisami prawa Unii lub przepisami krajowymi przyjętymi zgodnie z prawem Unii, a także z wszelkimi mającymi zastosowanie przepisami prawa krajowego, które są zgodne z prawem Unii i których nie można wyłączyć w drodze umowy.

9.6.2. Jeżeli jakiejkolwiek luki lub niejasności w niniejszej umowie nie można usunąć w sposób, o którym mowa w klauzuli 9.6.1, niniejszą umowę należy interpretować w świetle zasad wykładni przewidzianych w prawie właściwym (zob. klauzula 9.5).

9.7. **Rozstrzyganie sporów**

9.7.1. Strony uzgadniają, że dołożą wszelkich starań w celu polubownego rozstrzygania sporów i że przed wniesieniem sprawy do sądu przekażą spór do (*wstawić nazwę i dane kontaktowe konkretnego organu rozstrzygania sporów lub, w przypadku sporów mieszczących się w jego właściwości, wskazać dowolny organ rozstrzygania sporów w państwie członkowskim spełniający warunki określone w art. 10 aktu w sprawie danych*).

[WARIANT] [Sądy (*określić państwo członkowskie*) będą miały wyłączną właściwość do rozpoznania sprawy dotyczącej niniejszej umowy.]

Dodatek 1

(dowody dotyczące wniosku oraz, w stosownych przypadkach, udzielonego umocowania)

[do opracowania przez strony]

Dodatek 2

(szczegółowe informacje dotyczące danych objętych umową oraz ustaleń dotyczących dostępu)

W tym dodatku strony powinny podać szczegółowe informacje dotyczące danych objętych umową, ustaleń dotyczących dostępu oraz środków i informacji niezbędnych do uzyskania dostępu do danych i ich wykorzystywania, zgodnie z uzgodnieniami w klauzulach 3.1 i 3.2.

Dodatek ten zawiera jedynie wykaz kluczowych elementów, które strony powinny uzgodnić. Strony powinny dostosować zarówno jego formę, jak i treść, tak aby odpowiadały ich potrzebom. Strony mogą w szczególności uzupełnić niniejszy wykaz.

A. **Specyfikacja treści danych**

W dodatku należy uporządkować i wyszczególnić objęte umową dane z produktu oraz dane z usług powiązanych, wskazując treść danych i częstotliwość ich zbierania (w postaci ustrukturyzowanego wykazu punktów danych lub precyzyjnie określonych kategorii danych).

B. **Okres zatrzymywania danych**

W dodatku powinien być wskazany okres zatrzymywania, tak aby użytkownik był poinformowany o czasie dostępności danych. Można to zrobić w sposób szczegółowy w odniesieniu do każdego punktu danych lub każdej grupy punktów danych.

C. **Szczegółowe uregulowania dotyczące danych**

W dodatku powinno być określone, czy całość lub część danych stanowi dane objęte szczegółowymi uregulowaniami. Można na przykład wskazać, czy i jakie dane kwalifikują się jako dane osobowe.

D. **Struktura i format danych**

W dodatku powinno być określone, w jakim ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego udostępnia się dane.

E. **Nośnik do przekazania danych lub udzielenia dostępu do danych**

W dodatku powinno być określone, za pomocą jakiego bezpiecznego i wygodnego nośnika elektronicznego posiadacz danych udostępni dane odbiorcy danych w drodze przekazania albo udzielenia dostępu.

F. **Czas dostępu do danych**

W dodatku powinny być określone szybkość, częstotliwość i inne związane z czasem parametry dostępu do danych, takie jak na przykład dostęp w czasie rzeczywistym, w czasie zbliżonym do rzeczywistego, w sposób ciągły, bez zbędnej zwłoki lub z określoną częstotliwością.

G. **Data rozpoczęcia**

W dodatku powinna być określona data rozpoczęcia, począwszy od której posiadacz danych będzie udostępniał dane odbiorcy danych.

H. **Informacje niezbędne do wykonywania praw dostępu przysługujących odbiorcy danych**

W tym miejscu w dodatku można określić informacje niezbędne do umożliwienia odbiorcy danych korzystania z przysługujących mu praw dostępu. Mogą one obejmować dane osoby wyznaczonej do kontaktów w celu rozwiązywania problemów technicznych zarówno po stronie posiadacza danych, jak i po stronie odbiorcy danych.

Dodatek 3

(dowody dotyczące wielkości odbiorcy danych i szczegółowe informacje dotyczące obliczania rekompensaty)

[do opracowania przez strony]

Dodatek 4

(tajemnice przedsiębiorstwa)

[do opracowania przez strony]

ZAŁĄCZNIK V

MODELOWE POSTANOWIENIA UMOWNE

na potrzeby umów dotyczących dzielenia się danymi między osobami dzielącymi się danymi a odbiorcami danych na zasadzie dobrowolności

Te modelowe postanowienia umowne opracowano na potrzeby umów, w których dzielenie się danymi między osobą dzielącą się danymi a odbiorcą danych odbywa się na zasadzie dobrowolności, tj. osoba dzieląca się danymi nie jest zobowiązana do dzielenia się danymi na podstawie rozporządzenia (UE) 2023/2854 (zwanego dalej „aktem w sprawie danych") ani na podstawie jakiegokolwiek innego obowiązku prawnego przewidzianego w prawie Unii (takiego jak art. 6 ust. 9 i 10 aktu o rynkach cyfrowych) lub prawie krajowym.

Główną nowością aktu w sprawie danych w odniesieniu do takich stosunków jest wprowadzenie w jego art. 13 mechanizmu kontroli nieuczciwych postanowień umownych. Postanowienia umowne dotyczące dostępu do danych i ich wykorzystywania lub odpowiedzialności oraz środków ochrony prawnej w przypadku naruszenia lub wygaśnięcia obowiązków dotyczących danych, które zostały jednostronnie nałożone na przedsiębiorstwo przez inne przedsiębiorstwo, nie są wiążące, jeżeli są nieuczciwe.

Chociaż niniejsza umowa nie ma na celu zastąpienia już istniejących umów dotyczących dzielenia się danymi na zasadzie dobrowolności, może ona służyć jako punkt odniesienia przy ocenie uczciwości klauzul zawartych w obowiązujących umowach.

W przypadkach obowiązkowego dzielenia się danymi w odniesieniu do danych z produktu oraz danych z usługi powiązanej na podstawie aktu w sprawie danych należy stosować „Modelowe postanowienia umowne na potrzeby umów między posiadaczami danych a odbiorcami danych o udostępnianie danych na wniosek użytkowników produktów skomunikowanych i usług powiązanych" (art. 5 aktu w sprawie danych) albo „Modelowe postanowienia umowne na potrzeby umów o dostęp do danych i ich wykorzystywanie zawieranych między posiadaczami danych a użytkownikami produktów skomunikowanych i usług powiązanych" (art. 4 aktu w sprawie danych).

Strony powinny zająć się oddzielnie innymi scenariuszami obowiązkowego dzielenia się danymi, zapewniając przestrzeganie zarówno obowiązków na podstawie szczególnego przepisu prawnego, jak i obowiązków wynikających z rozdziału III aktu w sprawie danych. Do takiego scenariusza obowiązkowego dzielenia się danymi mogą mieć zastosowanie specjalne zestawy postanowień opracowane przez Komisję Europejską lub przez państwo członkowskie.

1. **Strony umowy**

Niniejsza umowa o dostępie do danych i ich wykorzystywaniu zostaje zawarta między

(*wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia*) („osoba dzieląca się danymi")

a

(*wstawić nazwę/imię i nazwisko, dane kontaktowe i dalsze odniesienia*) („odbiorca danych")

zwanymi w niniejszej umowie łącznie „stronami", a każda indywidualnie „stroną".

Osobą dzielącą się danymi może być każde przedsiębiorstwo, które:

— posiada dane oraz

— ma prawo do dzielenia się danymi na zasadzie dobrowolności oraz

— w zależności od przypadku, sprawuje kontrolę nad charakterystyką danych lub nad środkami dostępu do danych w taki sposób, aby było w stanie wywiązać się z zobowiązań przewidzianych w niniejszych modelowych postanowieniach umownych (w przeciwnym razie inna umowa może być bardziej odpowiednia).

Należy pamiętać, że w przypadku dzielenia się danymi osobowymi wymagane jest przestrzeganie obowiązujących przepisów o ochronie danych (w tym istnienie podstawy prawnej, a także – w przypadku gdy dane są udostępniane odbiorcy danych w państwie trzecim – zgodność z wymogami dotyczącymi międzynarodowego przekazywania danych).

W odniesieniu do przypadków użycia związanych z aktem w sprawie danych osobą dzielącą się danymi może być na przykład:

— posiadacz danych na podstawie art. 2 pkt 13 rozporządzenia (UE) 2023/2854, który ma prawo do dzielenia się danymi z produktów i danymi z usług powiązanych lub który chce dzielić się danymi wywiedzionymi lub wywnioskowanymi;

— użytkownik produktu skomunikowanego lub usługi powiązanej, któremu posiadacz danych przekazał dane (w tym na przykład dane pochodzące od wirtualnego asystenta wchodzącego w interakcję z produktem lub usługą powiązaną);
— były odbiorca danych na podstawie art. 2 pkt 14 rozporządzenia (UE) 2023/2854, który ma obecnie prawo do wykorzystywania i udostępniania danych zgodnie z umowami zawartymi z użytkownikiem i posiadaczem danych.

W innych przypadkach użycia osobą dzielącą się danymi może być na przykład:

— rolnik, który chce dzielić się danymi dotyczącymi gleby ze swoim dostawcą AI w celu poprawy schematów upraw lub z innym dostawcą AI – w celu trenowania, ulepszania lub rozwoju nowych systemów AI;

— przedsiębiorstwo, które chce sprzedać część swoich danych biznesowych innemu przedsiębiorstwu;

— uniwersytet, który chce sprzedać dane instytutowi badań socjologicznych w celu tworzenia statystyk;

— przedsiębiorstwo IT, które chce uczestniczyć w sieci danych dotyczących incydentów cyberbezpieczeństwa w celu skrócenia czasu reagowania na incydenty.

Odbiorcą danych może być każde przedsiębiorstwo, któremu osoba dzieląca się danymi udostępnia dane i które otrzymuje oraz wykorzystuje dane do własnych celów biznesowych w zakresie niniejszej umowy jako druga strona umowy wobec osoby dzielącej się danymi.

Definicja odbiorcy danych zawarta w niniejszej umowie obejmuje każdą stronę otrzymującą dane w ramach dowolnego rodzaju dzielenia się danymi, a nie wyłącznie odbiorców danych w ramach scenariuszy obowiązkowego dzielenia się danymi przewidzianych w akcie w sprawie danych.

2. **Dane objęte umową**

Dane objęte niniejszą umową obejmują dane określone w **dodatku 1** („dane"). Jeżeli wszystkie dane przekazane na podstawie niniejszej umowy lub ich część są objęte szczegółowymi uregulowaniami (z wyjątkiem danych osobowych, o których wyraźnie mowa w klauzuli 3.2), osoba dzieląca się danymi zobowiązuje się do zidentyfikowania takich danych w **dodatku 2**, a także do stosowania odpowiednich środków w celu ochrony takich danych zgodnie z mającymi zastosowanie uregulowaniami.

Identyfikacja szczegółowych uregulowań

Ponieważ te postanowienia dotyczą wyłącznie dobrowolnego dzielenia się danymi, osoba dzieląca się danymi nie ma obowiązku dzielenia się jakimikolwiek danymi objętymi specjalnymi uregulowaniami prawnymi (w szczególności – i w przeciwieństwie do obowiązkowego dzielenia się danymi na podstawie aktu w sprawie danych – nie istnieje obowiązek dzielenia się danymi chronionymi jako tajemnica przedsiębiorstwa). Jeżeli dane objęte szczegółowymi uregulowaniami nie są udostępniane, nie muszą być wymienione w dodatku 2; jeżeli jednak są one udostępniane, należy je wymienić i odpowiednio chronić.

Dane wskazane jako takie w dodatku 2 mogą być na przykład:

— chronione jako tajemnica przedsiębiorstwa przez osobę dzielącą się danymi, w którym to przypadku będą objęte klauzulą dotyczącą tajemnic przedsiębiorstwa;

— uznane za poufne przez osobę dzielącą się danymi, w którym to przypadku będą chronione na podstawie klauzuli dotyczącej poufności;

— chronione prawami *sui generis* do baz danych lub innymi prawami własności intelektualnej, w którym to przypadku zastosowanie będzie miała klauzula dotycząca własności intelektualnej;

— objęte przepisami sektorowymi (np. dotyczącymi energii, obronności, bezpieczeństwa, finansów, badań klinicznych itp.), w tym przepisami dotyczącymi wspólnych europejskich przestrzeni danych;

— objęte ograniczeniami wynikającymi z prawa konkurencji lub

— chronione jakimikolwiek innymi odpowiednimi uregulowaniami prawnymi, które strony chciałyby wskazać.

Opis danych objętych odpowiednimi uregulowaniami prawnymi należy uzupełnić o informacje niezbędne do zgodnego z prawem i bezpiecznego wykorzystywania danych przez odbiorcę danych (np. w przypadku ochrony własności intelektualnej, informacji dotyczących licencjonowania i praw autorskich osób trzecich).

Szczególny przypadek wspólnych europejskich przestrzeni danych

W niektórych sytuacjach można dopuścić dzielenie się danymi w kontekście wspólnej europejskiej przestrzeni danych właściwej dla danej dziedziny. Takie dzielenie się danymi powinno być realizowane zgodnie z przepisami właściwego rozporządzenia mającego zastosowanie do takiej przestrzeni danych, w przypadku gdy dotyczy ono obowiązkowego dzielenia się danymi na podstawie tego rozporządzenia. Poza zakresem obowiązkowego dzielenia się danymi na podstawie właściwego rozporządzenia mającego zastosowanie do danej przestrzeni danych nadal jest możliwe dzielenie się danymi na zasadzie dobrowolności. W takim przypadku można stosować niniejszy zestaw postanowień.

3. **Podstawa umowy**

3.1. **Pochodzenie danych**

3.1.1. Osoba dzieląca się danymi niniejszym oświadcza, że dane dostarczone na podstawie niniejszej umowy pochodzą z następujących źródeł: *(wskazać wszystkie źródła danych oraz, w miarę możliwości, dane dostarczone przez każde ze źródeł)*

Strony mogą wskazać różne rodzaje źródeł, takie jak na przykład:

— dane z produktu lub dane z usługi powiązanej w rozumieniu aktu w sprawie danych;

— inne dane pochodzące z produktu lub usługi powiązanej, które nie kwalifikują się jako dane z produktu lub dane z usługi powiązanej w rozumieniu aktu w sprawie danych (np. dane wywnioskowane lub dane pochodzące z innego oprogramowania, takie jak dane demograficzne wprowadzone do aplikacji przez jej użytkownika);

— dane pochodzące ze źródeł zewnętrznych, na przykład dane przekazane osobie dzielącej się danymi przez osobę trzecią w odniesieniu do produktów lub użytkowników takiej osoby trzeciej;

— dane wytworzone przez osobę dzielącą się danymi (w sposób autonomiczny), na przykład rejestry klientów tworzone przez pracowników osoby dzielącej się danymi w jej systemie zarządzania relacjami z klientami, tabele, dane przetworzone, dane wywnioskowane, dane wywiedzione, dane połączone itp.

Gwarancje są co do zasady konsekwencją sytuacji, w której osoba dzieląca się danymi udostępnia dane, a odbiorca danych nie jest w stanie zweryfikować legalności tych danych ani ich pochodzenia. W takich przypadkach odbiorca danych musi polegać na osobie dzielącej się danymi i może chcieć uzyskać w tym zakresie określone gwarancje. Gwarancje mogą jednak nie być odpowiednie w sytuacji, w której to odbiorca danych znajduje się w lepszej pozycji do weryfikacji danych lub podjęcia ryzyka związanego z danymi – na przykład ze względu na fakt, że osoba dzieląca się danymi jest MŚP lub że dane są pobierane bezpośrednio z produktu.

3.1.2. Osoba dzieląca się danymi oświadcza, że:

a) (*w stosownych przypadkach*) ponieważ dane zawierają nieosobowe dane z produktu lub z usługi powiązanej (zdefiniowane w rozporządzeniu (UE) 2023/2854 w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania („akt w sprawie danych")), a osoba dzieląca się danymi na podstawie niniejszej umowy ma dostęp do danych w charakterze posiadacza danych, przetwarzanie takich danych oraz dzielenie się takimi danymi podlega – zgodnie z art. 4 ust. 13 aktu w sprawie danych – umowie z odpowiednim użytkownikiem, zgodnie z definicją w art. 2 pkt 12 aktu w sprawie danych („użytkownik"), a niniejsza umowa umożliwia dzielenie się danymi do celów przewidzianych w niniejszej umowie;

b) (*w stosownych przypadkach*) ponieważ dane zawierają dane z produktu lub dane z usługi powiązanej i osoba dzieląca się danymi w ramach niniejszej umowy uzyskała do nich dostęp w charakterze odbiorcy danych na podstawie art. 5 aktu w sprawie danych, niniejsza umowa nie narusza zobowiązań umownych wobec użytkownika i posiadacza danych ani obowiązków wynikających z aktu w sprawie danych;

c) jest właścicielem lub posiada wystarczający tytuł prawny do danych wynikający z przepisów lub z umowy bez jakiegokolwiek naruszenia praw osób trzecich oraz że nie toczy się wobec niej żadne postępowanie, które – w przypadku niekorzystnego rozstrzygnięcia – mogłoby mieć istotny niekorzystny wpływ na jej zdolność do udzielenia praw przyznanych na mocy niniejszej umowy;

d) z wyjątkiem przypadków określonych w **dodatku 2** oraz bez uszczerbku dla klauzuli 3.2, uzyskała oraz będzie utrzymywać przez okres obowiązywania i do celów niniejszej umowy, na własny koszt, wszystkie zgody, licencje i upoważnienia wymagane do dzielenia się danymi oraz do wykorzystywania danych przez odbiorcę danych, w odniesieniu do wszelkich danych uzyskanych od osoby trzeciej lub przez nią dostarczonych.

3.1.3. (*w stosownych przypadkach*) Ponieważ dane zawierają dane z produktu lub dane z usługi powiązanej (zdefiniowane w akcie w sprawie danych), a osoba dzieląca się danymi na podstawie niniejszej umowy uzyskała do nich dostęp zgodnie z art. 4 aktu w sprawie danych w charakterze użytkownika, odbiorca danych oświadcza, że nie został wskazany jako strażnik dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925 („akt o rynkach cyfrowych").

3.1.4. [WARIANT] [Każda ze stron zapewnia, aby wszystkie dane, pliki lub oprogramowanie przekazane drugiej stronie na podstawie niniejszej umowy były wolne od wszelkich wirusów, złośliwego oprogramowania, oprogramowania szantażującego lub innego szkodliwego kodu, który mógłby naruszyć integralność, bezpieczeństwo lub funkcjonowanie systemów drugiej strony.]

3.1.5. [WARIANT] [Każda ze stron zapewnia, aby wszystkie dane, pliki lub oprogramowanie przekazane drugiej stronie na podstawie niniejszej umowy pochodziły z działań związanych z gromadzeniem danych, które są zgodne z mającymi zastosowanie standardami *(wskazać: zawodowymi, etycznymi, branżowymi, w zakresie cyberbezpieczeństwa, badawczymi lub w zakresie AI)*.]

3.2. **Zgodność z przepisami o ochronie danych i prywatności**

3.2.1. W zakresie, w jakim dane kwalifikują się jako dane osobowe, każda ze stron oświadcza, że przestrzega przepisów rozporządzenia (UE) 2016/679 („RODO") oraz, w stosownych przypadkach, dyrektywy 2002/58/WE, a także wszelkich innych mających zastosowanie przepisów o ochronie danych.

3.2.2. W **dodatku 3** strony muszą wymienić szczegółowe informacje na temat tego, które dane kwalifikują się jako dane osobowe, a także określić odpowiednie obowiązki stron w odniesieniu do przetwarzania takich danych osobowych na podstawie niniejszej umowy.

Role stron i porozumienia na gruncie RODO

Pojęcie „danych osobowych" w rozumieniu RODO ma bardzo szeroki zakres. Obejmuje ono wszelkie dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby. Dane nieosobowe mogą stać się danymi osobowymi, na przykład gdy stanowią część mieszanego zbioru danych, w którym są połączone z nowymi danymi, a efekt tego połączenia umożliwia powiązanie danych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Może to również mieć miejsce w przypadku pojawienia się nowych zdolności w zakresie przetwarzania danych. Strony powinny dokonać oceny własnych ról na gruncie RODO.

Kluczowe pojęcia RODO:

— „osoba, której dane dotyczą" oznacza zidentyfikowaną lub możliwą do zidentyfikowania osobę fizyczną, której dotyczą informacje;

— „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

— „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Klauzule te mają zastosowanie, gdy osoba dzieląca się danymi jest administratorem lub współadministratorem wraz z inną stroną na podstawie RODO. Aby ustalić, kto pełni jaką rolę na mocy RODO, strony muszą rozważyć, czy to one decydują o tym, dlaczego (cel) oraz w jaki sposób (za pomocą jakich środków) przetwarza się dane osobowe.

— Jeżeli osoba dzieląca się danymi udostępnia dane odbiorcy danych, który wykorzystuje je do własnych celów, obie strony są odrębnymi administratorami i ponoszą niezależną odpowiedzialność za przestrzeganie RODO.

— Jeżeli natomiast osoba dzieląca się danymi udostępnia dane odbiorcy danych w celu realizacji wspólnego celu, osoba dzieląca się danymi oraz odbiorca danych są współadministratorami na podstawie art. 26 RODO. W takim przypadku muszą oni wspólnie ustalić sposób zapewnienia zgodności z RODO.

— W przypadku gdy do zapewnienia zgodności z RODO potrzebne są dodatkowe klauzule umowne (np. na podstawie art. 26 lub art. 46), takie klauzule mogą (i powinny) być stosowane wraz z tymi modelowymi postanowieniami umownymi. Strony mogą się do nich odnieść w **dodatku 3**, który co do zasady powinien określać, w jaki sposób spełniane są wymogi przewidziane w RODO, w tym w szczególności w odniesieniu do ról i zakresu odpowiedzialności poszczególnych stron na gruncie RODO.

Ważna podstawa prawna

Zgodnie z art. 6 ust. 1 RODO powinna istnieć ważna podstawa prawna do dzielenia się danymi, a osobę, której dane dotyczą, należy poinformować o tym (dalszym) przetwarzaniu na podstawie art. 13 lub 14 RODO.

— Ważną podstawą prawną w przypadku, gdy osoba dzieląca się danymi oraz odbiorca danych działają jako dwaj odrębni administratorzy lub jako współadministratorzy, może być zgoda osoby, której dane dotyczą, umowa zawarta z tą osobą lub w jej interesie lub prawnie uzasadniony interes administratorów lub osoby trzeciej (o ile interes ten nie jest nadrzędny wobec interesów lub praw osoby, której dane dotyczą).

— Danymi można się dzielić wyłącznie w określonym, wyraźnym i prawnie uzasadnionym celu. Może to być na przykład dzielenie się danymi w celu ulepszania produktu, jeżeli strony uzgodniły, że dane będą wykorzystywane do wspólnego opracowania nowej funkcjonalności.

— Osoba dzieląca się danymi, działająca jako administrator, mogłaby również dzielić się danymi – ze względu na swój uzasadniony interes polegający na lepszym zatrzymywaniu klientów w przyszłości – ze swoją spółką dominującą, która również działa jako niezależny administrator i wykorzystuje dane do tworzenia statystyk globalnych – ze względu na swój prawnie uzasadniony interes polegający na poprawie usług świadczonych na całym świecie przez grupę.

Odbiorca danych powinien otrzymać od osoby dzielącej się danymi wystarczające informacje, aby móc wykazać zgodność z RODO. Na przykład strony mogą zgodzić się na podanie pierwotnego celu gromadzenia danych w **dodatku 3**. Może to być konieczne do ustalenia, czy przetwarzanie w innym celu jest zgodne z celem, w jakim dane osobowe zostały pierwotnie zebrane na podstawie art. 6 ust. 4 RODO, w przypadku współadministrowania. Wszystkie niezbędne szczegóły dotyczące odpowiednich obowiązków stron w zakresie przetwarzania takich danych osobowych na podstawie niniejszej umowy należy określić w **dodatku 3**.

Więcej informacji na temat RODO:

— wyjaśnienie kluczowych pojęć zawartych w RODO:

https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en?prefLang=pl;

— przewodnik dotyczący ochrony danych dla małych przedsiębiorstw:

https://www.edpb.europa.eu/sme-data-protection-guide/home_en;

— wytyczne, zalecenia i najlepsze praktyki Europejskiej Rady Ochrony Danych:

https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_pl;

— dodatkowe wskazówki można uzyskać od krajowych organów ochrony danych w każdym państwie członkowskim. Wykaz krajowych organów ochrony danych:

https://www.edpb.europa.eu/about-edpb/about-edpb/members_pl;

— standardowe klauzule umowne na podstawie art. 28 RODO:
https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en?prefLang=pl&etrans=pl;

— informacje dotyczące przekazywania danych osobowych poza UE/EOG:
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_pl.

3.3. **Nieprawidłowość oświadczeń**

3.3.1. Każda strona, która dowie się, że którekolwiek z oświadczeń, o których mowa w niniejszej klauzuli, nie jest lub przestało być prawidłowe lub przestanie być prawidłowe w dającej się przewidzieć przyszłości, bez zbędnej zwłoki powiadamia o tym drugą stronę, chyba że druga strona jest lub powinna być już świadoma tego faktu.

3.3.2. Po powzięciu wiadomości o takiej sytuacji dana strona musi podjąć odpowiednie działania i – w miarę możliwości – skorygować nieprawidłowość oświadczenia. Jeżeli sytuacja nie zostanie naprawiona i nie może zostać naprawiona, niniejsza umowa musi zostać rozwiązana w drodze pisemnego wypowiedzenia przekazanego przez jedną ze stron drugiej stronie, zawierającego przyczyny rozwiązania umowy. Rozwiązanie umowy następuje ze skutkiem natychmiastowym. W przypadku gdy nieprawidłowość dotyczy jedynie części danych objętych niniejszą umową, rozwiązanie wywołuje skutki wyłącznie w odniesieniu do tej części.

3.3.3. Dalsze skutki rozwiązania umowy reguluje klauzula 9.3.

4. Udostępnianie danych

4.1. Charakterystyka danych

Osoba dzieląca się danymi może podejmować różne stopnie zobowiązań w odniesieniu do przekazywanych danych, począwszy od najbardziej podstawowego zobowiązania polegającego na przekazywaniu danych wraz z metadanymi, tak aby były one zrozumiałe, a skończywszy na najbardziej rygorystycznym zobowiązaniu, zgodnie z którym dane będą odpowiadały celom przewidzianym przez odbiorcę danych lub będą wyczerpujące i prawidłowe. Strony mogą wybrać spośród poniższych wariantów.

Ponadto strony mogą dodać wszelkie dodatkowe wymogi, które mają sens z punktu widzenia konkretnej sytuacji w zakresie dzielenia się danymi: na przykład w przypadku dzielenia się danymi do celów badawczych, cel, jakim jest zapewnienie odtwarzalności badań naukowych, może wymagać określenia częstotliwości i okresu zatrzymywania każdej zaktualizowanej wersji zbioru danych, w którym to przypadku elementy te można dodać w sekcji „szczególne wymogi jakości" poniżej.

Osoba dzieląca się danymi udostępnia odbiorcy danych dane:

a) takiej samej jakości, w jakiej są one dostępne dla osoby dzielącej się danymi, oraz

b) wraz z odpowiednimi metadanymi, tabelami dziedzinowymi, semantyką, informacjami dotyczącymi licencji i innymi informacjami wymaganymi do tego, aby dane były zrozumiałe dla odbiorcy danych.

[WARIANT] c) [oraz *(wybrać jeden wariant lub więcej, stosownie do przypadku*)

(i) Dane są udostępniane w całościowym, ustrukturyzowanym, powszechnie używanym i nadającym się do odczytu maszynowego formacie. Strony uznają, że wymóg ten jest spełniony za pomocą następujących specyfikacji dotyczących danych: *(określić)*

(ii) Dane są udostępniane zgodnie z zasadami FAIR (możliwe do znalezienia, dostępne, interoperacyjne i nadające się do ponownego wykorzystania) opisanymi szczegółowo na stronie www.go-fair.org/fair-principles: [WARIANT] [(*opisać, w jaki sposób spełnić kryteria FAIR*)]

Przestrzeganie zasad FAIR można osiągnąć przez spełnienie szeregu wymiernych wymogów. Opracowany przez RDA model dojrzałości FAIR (https://publications.jrc.ec.europa.eu/repository/handle/JRC140764) zapewnia ramy służące do oceny stopnia, w jakim wskaźniki te są spełnione. Osoba dzieląca się danymi powinna dostosować swoje praktyki dzielenia się danymi do poziomu dojrzałości odpowiedniego dla jej szczególnych potrzeb.

Osoba dzieląca się danymi musi co najmniej zapewnić dostępność metadanych i ich zgodność ze wszystkimi wskaźnikami oznaczonymi w modelu dojrzałości jako „niezbędne". Ponadto osoba dzieląca się danymi może korzystać z narzędzi, dobrych praktyk i wytycznych dostosowanych do kontekstu, takich jak te dostępne na stronie https://doi.org/10.2760/5646214, w celu uproszczenia i skonkretyzowania wdrażania zasad FAIR.

(iii) Dane są dostosowywane do następującego kontekstu przetwarzania przez osobę dzielącą się danymi, zgodnie ze zwykłymi oczekiwaniami: (*dodać krótki opis*)

(iv) Dane są odpowiednie do celów realizowanych przez odbiorcę danych: (*dodać krótki opis*)

(v) Osoba dzieląca się danymi udostępnia odbiorcy danych: (*dodać/usunąć/uzupełnić szczególne wymogi jakości*)

— wyczerpujący zbiór danych, tj. dane zawierają wszystkie dane będące w posiadaniu osoby dzielącej się danymi objęte zakresem niniejszej umowy, lub

— aktualny zbiór danych, tj. dane odzwierciedlają dane będące w posiadaniu osoby dzielącej się danymi na dzień podpisania niniejszej umowy, lub

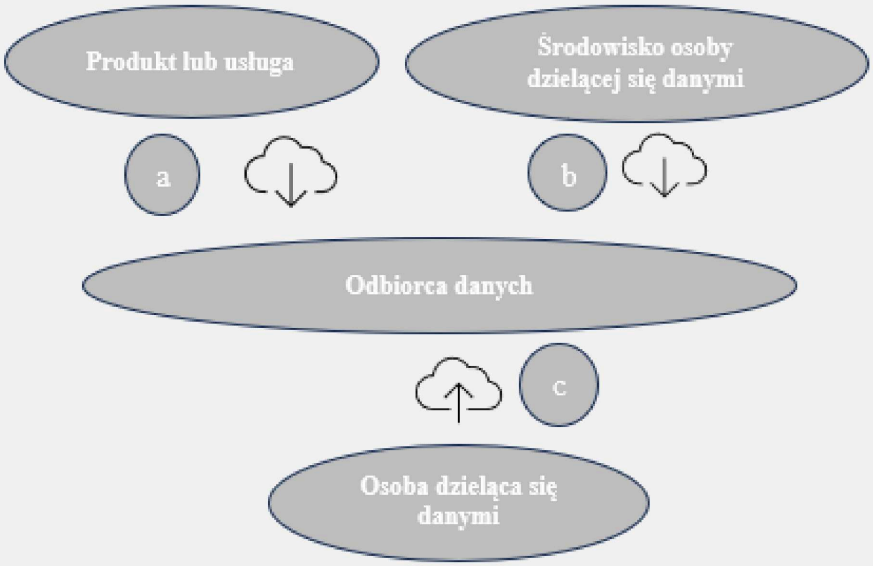
— dokładny zbiór danych, tj. dane wyselekcjonowała osoba dzieląca się danymi i – według jej najlepszej wiedzy – są one wolne od błędów, prawidłowe i wiarygodne, lub

— zbiór danych zgodny z następującymi standardami: *(określić np. interoperacyjności, dostępności, bezpieczeństwa itp.)*

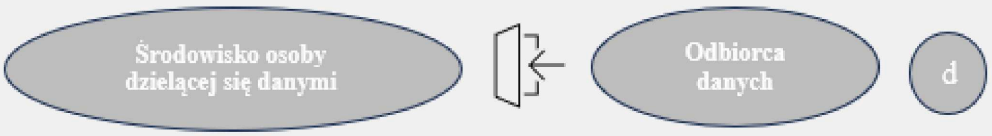
— zbiór danych dostępny w formacie otwartym, tj. w formacie, który nie jest zastrzeżony i może być używany przez każdego, a mianowicie: (*określić*)].

4.2. **Obowiązki osoby dzielącej się danymi w odniesieniu do dostępu do danych**

Osoba dzieląca się danymi może udostępniać dane na różne sposoby, przekazując albo zachowując kontrolę techniczną nad danymi (bez uszczerbku dla przyznanych lub zachowanych praw własności intelektualnej). Strony mogą na przykład uzgodnić, że odbiorca danych pobiera dane z produktu lub usługi (wariant a) lub ze środowiska osoby dzielącej się danymi (wariant b) lub że osoba dzieląca się danymi przekazuje dane do środowiska odbiorcy danych (wariant c).



Strony mogą również uzgodnić, że dane nie będą przekazywane odbiorcy danych, lecz zostaną udostępnione do przetwarzania w środowisku osoby dzielącej się danymi. Byłoby to szczególnie istotne w sytuacji dotyczącej danych osobowych (wariant d).



Przy udostępnianiu danych w ramach jednego lub kilku wariantów strony muszą wdrożyć różne środki bezpieczeństwa danych w celu zapewnienia początkowej i bieżącej poufności, integralności oraz dostępności danych. Oprócz zabezpieczeń prawnych dotyczących danych osobowych, które opisano w klauzuli 3.2 (odpowiednio w dodatku 3), środki bezpieczeństwa (opisane szerzej w dodatku 4) powinny również obejmować aspekty techniczne i organizacyjne dotyczące na przykład:

— zapewniania poufności danych przez kontrolę dostępu oraz bezpieczny przepływ danych,

— postanowień dotyczących zatrzymywania danych oraz usuwania danych,

— środków zapewniających integralność danych oraz środków monitorowania,

— postanowień dotyczących naruszeń ochrony danych osobowych.

4.2.1. Osoba dzieląca się danymi udostępnia dane odbiorcy danych przez:

a) [WARIANT: pobieranie przez odbiorcę danych z produktów lub usług] [umożliwianie pobierania danych bezpośrednio z następujących produktów lub usług, które nie są hostowane przez osobę dzielącą się danymi, w tym przez udostępnienie wszelkich wymaganych specyfikacji technicznych (np. protokołu komunikacyjnego) na następujących warunkach technicznych: (*wstawić metodę oraz produkty/usługi, które nie są hostowane przez osobę dzielącą się danymi*);]

b) [WARIANT: pobieranie przez odbiorcę danych ze środowiska osoby dzielącej się danymi] [umożliwianie pobierania danych ze środowiska osoby dzielącej się danymi, w tym przez udostępnianie wszelkich wymaganych specyfikacji technicznych, na następujących warunkach technicznych: (*wstawić metodę, np. pobieranie plików lub korzystanie z API (interfejsu programowania aplikacji) w celu interakcji z usługami osoby dzielącej się danymi*);]

(*ma zastosowanie, jeżeli wybrano wariant a lub b*) [Osoba dzieląca się danymi niniejszym upoważnia odbiorcę danych do korzystania ze specyfikacji wyłącznie w celu pobierania danych, w zakresie określonym w niniejszej umowie. Odbiorca danych zgadza się i potwierdza, że z wyjątkiem powyższego prawa nie przysługuje mu żadne inne prawo, interes ani licencja do specyfikacji.]

c) [WARIANT: przekazanie danych przez osobę dzielącą się danymi do środowiska odbiorcy danych] [zapewnienie pełnego przekazania danych ze środowiska osoby dzielącej się danymi do środowiska odbiorcy danych, na następujących warunkach technicznych: *(wstawić metodę, np. jednorazowe przekazanie lub regularne przekazywanie plików zip odbiorcy danych)*;]

d) [WARIANT: dostęp odbiorcy danych do środowiska osoby dzielącej się danymi] [zapewnienie dostępu do danych w środowisku osoby dzielącej się danymi na następujących warunkach technicznych: *(wstawić metodę, np. logowanie do platformy, dozwolone funkcje, w tym funkcje eksportu, w zależności od przypadku)*;]

Osoba dzieląca się danymi niniejszym przyznaje odbiorcy danych niezbywalne, bez prawa do udzielania sublicencji, prawo dostępu do danych w środowisku opisanym powyżej wyłącznie w celu i na okres, jakie określono w niniejszej umowie. Osoba dzieląca się danymi zastrzega sobie prawo do zawieszenia dostępu do tego środowiska w przypadku wykrycia niezgodnego z umową wykorzystania danych.

4.2.2. Do celów klauzuli 4.2.1 uznaje się, że środowisko osoby dzielącej się danymi i środowisko odbiorcy danych obejmują:

a) środowisko każdej osoby trzeciej wyznaczonej przez daną stronę do przechowywania lub otrzymywania danych w jej imieniu (w tym – w stosownych przypadkach – bezpieczne środowisko przetwarzania zdefiniowane w art. 2 pkt 20 rozporządzenia (UE) 2022/868);

b) wszelkie aplikacje lub oprogramowanie hostowane przez daną stronę bezpośrednio lub za pośrednictwem usługodawców.

W przypadkach, w których mają zostać opracowane zastosowania uczenia maszynowego lub AI, w celu zapewnienia odbiorcy danych dostępu do danych w sposób zapewniający ochronę prywatności można wykorzystać nowatorskie technologie, takie jak uczenie federacyjne i prywatność różnicowa, opisane bardziej szczegółowo na stronie https://publications.jrc.ec.europa.eu/repository/handle/JRC141298.

W przypadku uczenia federacyjnego dane są „odwiedzane" przez algorytm odbiorcy danych, który jest wykonywany w bezpiecznym środowisku przetwarzania osoby dzielącej się danymi lub osoby trzeciej. Podejście to zapobiega uzyskaniu przez odbiorcę danych bezpośredniego dostępu do danych oraz ich bezpośredniej widoczności. W przypadku prywatności różnicowej do pierwotnych danych dodaje się szum w celu ochrony niektórych wrażliwych cech.

4.2.3. Osoba dzieląca się danymi udostępnia dane odbiorcy danych zgodnie z następującymi wymogami dotyczącymi czasu lub harmonogramu: (*wstawić czas, np. codziennie, o określonej godzinie, częstotliwość, w czasie rzeczywistym lub szczegółowy harmonogram lub termin*)

[WARIANT] [Jeżeli w okresie obowiązywania niniejszej umowy osoba dzieląca się danymi wejdzie w posiadanie zaktualizowanej lub skorygowanej wersji danych, zobowiązuje się do udostępnienia takiej zaktualizowanej lub skorygowanej wersji odbiorcy danych bez zbędnej zwłoki po jej udostępnieniu osobie dzielącej się danymi. W przypadku gdy dane są stale aktualizowane i korygowane, będą one udostępniane odbiorcy danych *(określić: codziennie/co tydzień/co miesiąc)*.]

[WARIANT] Osoba dzieląca się danymi zapewni, aby każda nowa wersja zbioru danych była prawidłowo oznakowana, a wcześniejsze wersje pozostały dostępne odbiorcy danych przez okres obowiązywania niniejszej umowy oraz przez okres *(określić)* po jej zakończeniu.

[WARIANT] Dane są zatrzymywane przez osobę dzielącą się danymi przez okres *(określić)*, po upływie którego nie będą już dostępne dla odbiorcy danych.

4.2.4. Osoba dzieląca się danymi musi zapewnić odbiorcy danych środki i informacje niezbędne do uzyskania dostępu do danych lub ich otrzymania zgodnie z niniejszą umową. Obejmuje to w szczególności:

a) [WARIANT – w przypadku gdy dane nie są dostarczane w standardowym formacie] [dostarczenie oprogramowania oraz towarzyszącej licencji wymaganych do wykorzystywania danych w uzgodnionym celu, które to dane nie są łatwo dostępne na rynku, lecz mogą zostać dostarczone przez osobę dzielącą się danymi, lub mapowanie dostępnego formatu na otwartą i powszechnie używaną specyfikację lub otwarty i powszechnie używany słownik pojęć;]

b) udostępnianie osobie dzielącej się danymi łatwo dostępnych informacji na temat pochodzenia danych i wszelkich praw, jakie mogą przysługiwać osobom trzecim w odniesieniu do danych, lub okoliczności, jakie mogą prowadzić do powstania takich praw.

[WARIANT] Strony niniejszym uzgadniają, że środki i informacje, o których mowa powyżej, obejmują: *(określić)*.

4.3. **Obowiązki odbiorcy danych w odniesieniu do dostępu do danych**

4.3.1. Odbiorca danych przekazuje osobie dzielącej się danymi informacje techniczne i odpowiednie dane niezbędne do tego, aby osoba dzieląca się danymi mogła spełnić wymagania określone powyżej.

4.3.2. (w stosownych przypadkach w przypadku dostępu do danych w środowisku osoby dzielącej się danymi) Odbiorca danych:

a) zapewni, aby wyłącznie pracownicy, którzy pracują dla odbiorcy danych lub z nim współpracują oraz których obowiązki wymagają dostępu do danych w celu wykonania niniejszej umowy (zasada ograniczonego dostępu), mogli uzyskiwać dostęp do środowiska osoby dzielącej się danymi, a pracownicy ci będą przestrzegać niniejszej umowy, dodatków do niej oraz mających zastosowanie przepisów;

b) nie będzie:

(i) upoważniać żadnej osoby trzeciej do dostępu ani umożliwiać żadnej osobie trzeciej dostępu do środowiska osoby dzielącej się danymi;

(ii) tworzyć utworów zależnych ani uzyskiwać dostępu do środowiska osoby dzielącej się danymi w celu opracowania jakiegokolwiek konkurencyjnego produktu lub konkurencyjnej usługi ani w celu kopiowania jakiegokolwiek elementu, jakiejkolwiek funkcji lub jakiegokolwiek wykresu w środowisku osoby dzielącej się danymi;

(iii) kopiować, replikować, poddawać inżynierii odwrotnej, dekompilować, rozkładać na części ani podejmować prób wydobycia jakiegokolwiek kodu źródłowego, algorytmów, metod lub technik stosowanych w środowisku osoby dzielącej się danymi [WARIANT] [z wyjątkiem zakresu ściśle wymaganego do badania kompatybilności lub optymalizacji na potrzeby integracji];

(iv) obchodzić ani omijać jakichkolwiek mechanizmów bezpieczeństwa środowiska osoby dzielącej się danymi ani

(v) wykorzystywać środowiska technicznego osoby dzielącej się danymi w celu uzyskania dostępu do danych innych niż dane objęte niniejszą umową lub na warunkach odmiennych od określonych w niniejszej umowie.

4.4. **Środki bezpieczeństwa**

4.4.1. Każda ze stron zapewnia poufność, integralność oraz dostępność danych przez wdrożenie odpowiednich środków bezpieczeństwa opisanych w **dodatku 4**, w przypadku udostępniania danych w ramach ustaleń dotyczących dostępu, o których mowa w klauzuli 4.2.1.

4.4.2. Jeżeli zmiany w danych lub w ich środowisku mogą mieć wpływ na bezpieczeństwo danych, osoba dzieląca się danymi oraz odbiorca danych zgadzają się na ocenę środków bezpieczeństwa (*określić: regularnie/na wniosek drugiej strony/w przypadku wystąpienia szczególnych zdarzeń*) oraz negocjacje w dobrej wierze w sprawie wszelkich niezbędnych dostosowań.

4.4.3. Każda ze stron, na wniosek drugiej strony, przekazuje szczegółowe informacje na temat środków wykonawczych zastosowanych zgodnie z niniejszą klauzulą 4.4 oraz dodatkiem 4.

4.4.4. Każda ze stron zgłasza drugiej stronie każde naruszenie bezpieczeństwa prowadzące do przypadkowych lub niezgodnych z prawem zniszczenia, utraty, zmiany lub nieuprawnionego ujawnienia lub dostępu do danych w ciągu 24 godzin od ich wykrycia.

4.4.5. [WARIANT] [Osoba dzieląca się danymi zastrzega sobie prawo do przeprowadzania okresowych audytów lub żądania dokumentacji w celu weryfikacji zgodności z wymogami bezpieczeństwa nałożonymi na odbiorcę danych.]

4.4.6. (w stosownych przypadkach) Osoba dzieląca się danymi zobowiązuje się nie przechowywać żadnych informacji na temat dostępu odbiorcy danych do danych, których dotyczy wniosek, poza informacjami, które są niezbędne do zapewnienia:

a) dostępu do danych

b) (w stosownych przypadkach) bezpieczeństwa i utrzymania infrastruktury danych oraz

c) przestrzegania obowiązków prawnych osoby dzielącej się danymi.

Osoba dzieląca się danymi informuje odbiorcę danych o informacjach przechowywanych przez nią zgodnie z prawem właściwym lub na wniosek odbiorcy danych.

4.5. **Obowiązek renegocjacji, mechanizm informacji zwrotnej i jednostronne zmiany**

4.5.1. Jeżeli dane są udostępniane zgodnie z ustaleniami umownymi dotyczącymi charakterystyki danych, procedur dostępu lub niezbędnych środków i informacji umożliwiających dostęp do danych i ich wykorzystywanie oraz jeżeli okaże się, że uzgodnione ustalenia umowne są niewystarczające do uzyskania dostępu do danych i ich wykorzystywania w sposób przewidziany w niniejszej umowie, strony zobowiązują się do rozpoczęcia negocjacji w dobrej wierze i dostosowania ustaleń umownych.

4.5.2. Jeżeli odbiorca danych zidentyfikuje incydent związany z klauzulą 2 – dotyczącą danych objętych umową – lub klauzulami 4.1 i 4.2 – dotyczącymi charakterystyki danych i ustaleń dotyczących dostępu – oraz jeżeli odbiorca danych przekaże osobie dzielącej się danymi szczegółowy opis tego incydentu, osoba dzieląca się danymi i odbiorca danych muszą współpracować w dobrej wierze w celu zidentyfikowania przyczyny incydentu. Jeżeli incydent został spowodowany niedopełnieniem obowiązków przez osobę dzielącą się danymi, osoba ta jest zobowiązana usunąć naruszenie bez zbędnej zwłoki. Jeżeli osoba dzieląca się danymi nie usunie naruszenia, uznaje się to za istotne naruszenie zobowiązania, a odbiorca danych może powołać się na klauzulę 10 niniejszej umowy dotyczącą środków ochrony prawnej w przypadku naruszenia umowy.

4.5.3. Jeżeli osiągnięcie któregokolwiek z ustaleń umownych uzgodnionych zgodnie z klauzulami od 4.1 do 4.2 okaże się niemożliwe lub nadmiernie uciążliwe z powodu wyjątkowej zmiany okoliczności, która nastąpiła po zawarciu umowy, osoba dzieląca się danymi musi przedstawić odbiorcy danych szczegółowy opis tej sytuacji, a strony rozpoczną negocjacje w dobrej wierze i dostosują ustalenia umowne. W szczególności każda ze stron musi przekazać drugiej stronie wystarczające informacje, aby umożliwić ocenę, omówienie i rozwiązanie danej sytuacji. Niniejsza klauzula nie narusza prawa odbiorcy danych do skorzystania ze środków ochrony prawnej zgodnie z klauzulą 10.

4.5.4. Osoba dzieląca się danymi może, działając w dobrej wierze, jednostronnie zmienić szczegóły dotyczące ustaleń umownych w zakresie danych oraz ustaleń dotyczących dostępu, jeżeli jest to obiektywnie uzasadnione zwykłym prowadzeniem działalności gospodarczej przez osobę dzielącą się danymi, na przykład modyfikacją techniczną wynikającą z bezpośredniego zagrożenia bezpieczeństwa w odniesieniu do linii produktów lub usług powiązanych oferowanych przez osobę dzielącą się danymi lub zmianą infrastruktury osoby dzielącej się danymi. Każda zmiana musi spełniać podstawowe wymogi klauzul 4.1 i 4.2.

4.5.5. Osoba dzieląca się danymi musi zawiadomić odbiorcę danych o zmianie co najmniej (*wskazać rozsądny okres*) przed wejściem zmiany w życie.

Krótszy termin zawiadomienia może być wystarczający:

a) jeżeli zmiana nie ma negatywnego wpływu na dostęp do danych i ich wykorzystywanie przez odbiorcę danych lub

b) jeżeli takie zawiadomienie byłoby niemożliwe lub nierozsądne w danych okolicznościach, na przykład gdy natychmiastowe zmiany są wymagane ze względu na wykrycie bezpośredniego zagrożenia bezpieczeństwa.

W przypadku gdy zmiana negatywnie wpływa na dostęp odbiorcy danych do danych lub ich wykorzystywanie przez odbiorcę danych, strony zobowiązują się do współpracy w celu zmniejszenia takiego wpływu. Odbiorca danych może w każdym przypadku rozwiązać (odpowiednią część) umowy bez obowiązku zapłaty jakiejkolwiek rekompensaty na rzecz osoby dzielącej się danymi, niezależnie od innych praw lub środków ochrony prawnej przysługujących odbiorcy danych.

5. **Wykorzystywanie danych i dzielenie się danymi z osobami trzecimi**

5.1. **Wykorzystywanie danych**

5.1.1. Dozwolone cele (*wybrać tylko jeden wariant*)

[WARIANT OGRANICZAJĄCY] [Odbiorca danych może przetwarzać dane wyłącznie w następujących celach: (*określić dozwolone cele*) („dozwolone cele").]

lub

[WARIANT SZEROKI – wyłącznie w odniesieniu do danych nieosobowych] [Odbiorca danych może przetwarzać dane w dowolnym zgodnym z prawem celu („dozwolone cele") [WARIANT] [z wyjątkiem (*określić, np. wykorzystywania otrzymanych danych do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji lub wykorzystywania przez osobę dzielącą się danymi*)].]

(*w stosownych przypadkach, jeżeli dane obejmują dane z produktu lub dane z usługi powiązanej, a osoba dzieląca się danymi w ramach niniejszej umowy uzyskała do nich dostęp zgodnie z art. 4 lub 5 aktu w sprawie danych w roli użytkownika lub odbiorcy danych*) Odbiorca danych nie może w żadnym przypadku wykorzystywać otrzymanych danych do opracowania produktu, który konkuruje z produktem, z którego pochodzą dane.

Uzgadniając dozwolone cele, strony powinny uwzględnić wszelkie ograniczenia wynikające z prawa właściwego lub z ich zobowiązań umownych wobec osób trzecich. Na przykład jeżeli dane stanowią dane z produktu zgodnie z definicją w akcie w sprawie danych, a osoba dzieląca się danymi jest użytkownikiem produktu lub odbiorcą danych w rozumieniu aktu w sprawie danych, powinna ona przestrzegać zakazu opracowania produktu konkurencyjnego, o którym mowa w art. 4 ust. 10 oraz art. 6 ust. 2 lit. e) aktu w sprawie danych. Jeżeli osoba dzieląca się danymi będąca użytkownikiem tego rodzaju uzgodniła z posiadaczem danych szczególne ograniczenia swoich praw wynikających z aktu w sprawie danych, umowa powinna być z nimi zgodna.

5.1.2. Dozwolone operacje na danych (*wybrać tylko jeden wariant*)

[WARIANT OGRANICZAJĄCY] [Odbiorca danych może wykonywać na danych wyłącznie następujące operacje: (*określić dozwolone operacje, np. dostęp do danych oraz ich kopiowanie w celu tworzenia zagregowanych statystyk w odniesieniu do dozwolonych celów*) („dozwolone operacje").]

lub

[WARIANT SZEROKI – wyłącznie w odniesieniu do danych nieosobowych] [Odbiorca danych może wykonywać na danych wszelkie operacje zgodne z prawem („dozwolone operacje") [WARIANT] [z wyjątkiem (*określić, np. hostowania danych lub innego ich przekazywania lub udostępniania poza Unię Europejską lub podejmowania prób identyfikacji osób, których dane dotyczą*)]

(*w stosownych przypadkach, jeżeli dane obejmują dane z produktu lub dane z usługi powiązanej, a osoba dzieląca się danymi w ramach niniejszej umowy uzyskała do nich dostęp zgodnie z art. 4 lub 5 rozporządzenia (UE) 2023/2854 w swojej roli użytkownika lub odbiorcy danych*) Odbiorca danych nie może w żadnym przypadku wykorzystywać otrzymanych danych w sposób, który miałby niekorzystny wpływ na bezpieczeństwo produktu lub jakiejkolwiek usługi powiązanej.]

5.1.3. Ponadto odbiorca danych zobowiązuje się, że w celu uzyskania danych nie będzie:

a) przekazywać osobie dzielącej się danymi nieprawdziwych informacji,

b) stosować środków wprowadzających w błąd ani środków przymusu,

c) nadużywać luk ani wykorzystywać jakichkolwiek podatności w infrastrukturze technicznej osoby dzielącej się danymi mającej chronić dane.

5.1.4. Prawo do wykorzystywania danych zgodnie z niniejszą klauzulą przyznaje się odbiorcy danych (*określić: bezterminowo/przez cały okres obowiązywania umowy/przez okres (określić)*).

5.1.5. (*jeżeli ma to zastosowanie w przypadku pobierania danych przez odbiorcę danych lub przekazywania danych odbiorcy danych oraz jeżeli strony uzgodniły ograniczenie wykorzystywania danych w czasie*) Po rozwiązaniu umowy lub wygaśnięciu prawa do wykorzystywania danych odbiorca danych zobowiązuje się do trwałego usunięcia danych (w tym wszelkich kopii lub kopii zapasowych) oraz do zapewnienia, aby wszelkie osoby trzecie, którym ujawniono dane, trwale usunęły takie dane. Na wniosek osoby dzielącej się danymi odbiorca danych bez zbędnej zwłoki przekazuje pisemne potwierdzenie takiego usunięcia.

5.2. **Dzielenie się danymi z osobami trzecimi**

5.2.1. Odbiorca danych nie udostępnia ani nie przekazuje żadnych danych jakiejkolwiek osobie trzeciej, niezależnie od tego, czy dane te mają postać zidentyfikowaną, zanonimizowaną, spseudonimizowaną czy zagregowaną [WARIANT] [, z wyjątkiem sytuacji, w której odbiorca danych może dzielić się danymi wyłącznie w następującym celu ich wykorzystania: *(określić)*. Osoba trzecia nie dzieli się żadnymi danymi ani nie przekazuje żadnych danych dalej, [WARIANT] [z wyjątkiem następującego celu wykorzystania danych: (*określić*)]].

5.2.2. (w stosownych przypadkach, jeżeli dane zawierają dane z produktu lub dane z usługi powiązanej, a osoba dzieląca się danymi na podstawie niniejszej umowy uzyskała do nich dostęp zgodnie z art. 4 lub 5 aktu w sprawie danych w charakterze użytkownika lub odbiorcy danych) Odbiorca danych nie może udostępniać otrzymanych danych przedsiębiorstwu wskazanemu jako strażnik dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925 (akt o rynkach cyfrowych).

5.2.3. W przypadku gdy odbiorca danych jest uprawniony do udostępnienia danych osobie trzeciej na podstawie niniejszej umowy, odbiorca danych musi:

a) [WARIANT] [poinformować osobę dzielącą się danymi o fakcie, że dane zostaną udostępnione osobie trzeciej, wskazać dane, których to dotyczy, oraz przekazać osobie dzielącej się danymi informacje na temat tożsamości i dane kontaktowe tej osoby trzeciej;]

b) zastosować odpowiednie środki umowne, techniczne i organizacyjne w celu zapewnienia, aby osoba trzecia przestrzegała takich samych lub zasadniczo równoważnych zobowiązań jak odbiorca danych wynikających z niniejszej umowy. Obejmuje to w szczególności zobowiązania odbiorcy danych do:

(i) zapewnienia, aby osoba trzecia stosowała co najmniej takie same środki bezpieczeństwa i miała co najmniej takie same zobowiązania, jakie odbiorca danych uzgodnił w klauzuli „Środki bezpieczeństwa", oraz

(ii) zapewnienia, aby osoba trzecia wykorzystywała dane wyłącznie w sposób zgodny z klauzulą 5.1 dotyczącą wykorzystywania danych, oraz

(iii) [WARIANT] [zapewnienia, aby osobie dzielącej się danymi przysługiwały wobec osoby trzeciej co najmniej takie same środki ochrony prawnej w przypadku nieuprawnionego wykorzystania lub ujawnienia danych, jakie przysługują jej wobec odbiorcy danych na podstawie niniejszej umowy oraz]

(iv) (*jeżeli osoba trzecia jest uprawniona do dalszego udostępniania danych zgodnie z klauzulą 5.2.1*) [zobowiązania osoby trzeciej do zapewnienia, aby wszelkie kolejne osoby trzecie otrzymujące dane przestrzegały zobowiązań określonych w niniejszej umowie].

5.2.4. Niezależnie od klauzul od 5.2.1 do 5.2.3 odbiorca danych może – na własny rachunek i na własną odpowiedzialność – korzystać z usług przetwarzania danych, np. usług przetwarzania w chmurze (w tym infrastruktury jako usługi, platformy jako usługi i oprogramowania jako usługi), usług hostingu lub podobnych usług w celu wykorzystywania danych w sposób uzgodniony w klauzulach 5.1.1 i 5.2.1. Osoby trzecie mogą również – na własny rachunek i na własną odpowiedzialność – korzystać z takich usług w celu korzystania z danych w sposób uzgodniony w klauzuli 5.2.1.

6. **(jeżeli dane są chronione jako tajemnice przedsiębiorstwa) Tajemnice przedsiębiorstwa**

O tajemnicach przedsiębiorstwa

Tajemnice przedsiębiorstwa to informacje poufne, które zapewniają przedsiębiorstwu przewagę konkurencyjną.

Zgodnie z art. 2 pkt 1 dyrektywy (UE) 2016/943 termin „tajemnica przedsiębiorstwa" oznacza informacje, które spełniają trzy wymogi: a) są poufne w tym sensie, że jako całość lub w szczególnym zestawie i zbiorze ich elementów nie są ogólnie znane lub łatwo dostępne dla osób z kręgów, które zwykle zajmują się tym rodzajem informacji, b) mają wartość handlową dlatego, że są objęte tajemnicą oraz c) poddane zostały przez osobę, która zgodnie z prawem sprawuje nad nimi kontrolę, rozsądnym, w danych okolicznościach, działaniom dla utrzymania ich w tajemnicy.

„Posiadacz tajemnicy przedsiębiorstwa" oznacza każdą osobę fizyczną lub prawną, która w sposób zgodny z prawem sprawuje kontrolę nad taką tajemnicą przedsiębiorstwa.

W odniesieniu do danych osoba dzieląca się danymi może korzystać z ochrony tajemnicy przedsiębiorstwa w szczególności wówczas, gdy informacje cyfrowe obejmują:

— informacje techniczne (technologię produktu, dane z zakresu badań i rozwoju, wiedzę fachową na temat procesów, technologie nieopatentowane itp.);

— informacje handlowe (strategie rynkowe, informacje finansowe itp.).

W związku z tym – w odniesieniu do informacji cyfrowych – osoba dzieląca się danymi powinna zidentyfikować potencjalną tajemnicę przedsiębiorstwa. Więcej informacji na temat tajemnic przedsiębiorstwa w sektorze cyfrowym można znaleźć w przewodniku WIPO dotyczącym tajemnic przedsiębiorstwa i innowacji:

https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html

Ograniczony dostęp dla innych osób, szyfrowanie lub umowy o zachowanie poufności mogą stanowić metody zachowania poufności danych, a tym samym umożliwiać objęcie ich ochroną jako tajemnicy przedsiębiorstwa.

Jak postępować z tajemnicami przedsiębiorstwa?

Jeżeli osoba dzieląca się danymi zidentyfikuje określone tajemnice przedsiębiorstwa jako wchodzące w zakres dzielenia się danymi na podstawie umowy, nie jest ona zobowiązana do dzielenia się takimi danymi – w odróżnieniu od sytuacji przewidzianych w art. 4 ust. 6 oraz art. 5 ust. 9 aktu w sprawie danych.

Jeżeli osoba dzieląca się danymi zdecyduje się jednak na dzielenie się takimi danymi, może ustanowić i uzgodnić z odbiorcą danych określone wymogi jako warunek dzielenia się danymi chronionymi jako tajemnice przedsiębiorstwa, w szczególności obowiązek zastosowania dodatkowych środków technicznych i organizacyjnych w celu zachowania poufności. Osoba dzieląca się danymi i odbiorca danych powinni zawrzeć wszystkie szczegółowe informacje dotyczące danych, które są chronione jako tajemnice przedsiębiorstwa, w **dodatku 2** stanowiącym część umowy.

6.1. **Stosowanie ustaleń dotyczących tajemnic przedsiębiorstwa**

6.1.1. Środki ochrony a także powiązane prawa uzgodnione poniżej mają zastosowanie wyłącznie do danych lub metadanych zawartych w danych, które mają być udostępniane odbiorcy danych przez osobę dzielącą się danymi i które są chronione jako tajemnice przedsiębiorstwa (zgodnie z definicją zawartą w art. 2 pkt 1 dyrektywy (UE) 2016/943 w sprawie tajemnic przedsiębiorstwa), będących w posiadaniu posiadacza danych lub innego posiadacza tajemnicy przedsiębiorstwa (zgodnie z definicją zawartą w art. 2 pkt 2 tej dyrektywy).

6.1.2. Dane chronione jako tajemnice przedsiębiorstwa oraz tożsamość posiadacza tajemnicy przedsiębiorstwa określono w **dodatku 2**.

6.1.3. Zobowiązania określone w klauzulach 6.2 i 6.3 pozostają w mocy po każdym rozwiązaniu umowy, chyba że strony postanowią inaczej.

6.2. **Środki ochrony stosowane przez odbiorcę danych**

Odbiorca danych stosuje środki ochrony określone w **dodatku 4** (zwane dalej „środkami ochrony leżącymi w gestii odbiorcy danych").

W **dodatku 4** strony powinny zawrzeć wszystkie szczegółowe informacje na temat środków ochrony. Środki mogą mieć zarówno charakter techniczny (np. szyfrowanie, zapory sieciowe, przechowywanie danych w odrębnych lokalizacjach itp.), jak i organizacyjny (np. zarządzanie wewnętrzne, odpowiednie zarządzanie tożsamością i kontrole dostępu, zaangażowanie zaufanej osoby trzeciej).

Ponieważ środki muszą być proporcjonalne, ich treść będzie się różnić w zależności od charakteru tajemnicy przedsiębiorstwa. Środki te będą również zależały od tego, czy (i) udziela się dostępu do danych w miejscu ich przechowywania lub czy będzie to (ii) pełne przekazanie danych odbiorcy danych. W pierwszym przypadku posiadacz danych zachowuje wyższy stopień kontroli i może samodzielnie stosować część środków ochrony, podczas gdy odbiorca danych może mieć bardziej ograniczony zakres korzystania z danych. W każdym przypadku obie strony powinny koncentrować się na osiągnięciu zamierzonych skutków umowy.

6.3. **Środki ochrony stosowane przez posiadacza tajemnicy przedsiębiorstwa**

6.3.1. Osoba dzieląca się danymi może stosować środki uzgodnione w dodatku 4 w celu zachowania poufności danych chronionych jako tajemnice przedsiębiorstwa (zwane dalej „środkami ochrony stosowanymi przez osobę dzielącą się danymi").

6.3.2. Osoba dzieląca się danymi może również jednostronnie wprowadzić odpowiednie techniczne i organizacyjne środki ochrony, jeżeli nie mają one negatywnego wpływu na dostęp do danych i ich wykorzystywanie przez odbiorcę danych na podstawie niniejszej umowy.

6.3.3. Odbiorca danych zobowiązuje się nie zmieniać ani nie usuwać środków ochrony osoby dzielącej się danymi ani środków stosowanych zgodnie z klauzulą 6.3.2, chyba że strony postanowią inaczej.

6.4. **Posiadacze zidentyfikowanych tajemnic przedsiębiorstwa będący osobami trzecimi**

6.4.1. Osoba dzieląca się danymi oświadcza odbiorcy danych, że uzyskała wszystkie odpowiednie prawa od posiadaczy tajemnic przedsiębiorstwa będących osobami trzecimi do zawarcia niniejszej umowy w odniesieniu do danych chronionych jako tajemnice przedsiębiorstwa.

6.4.2. Środki ochrony odbiorcy danych oraz środki ochrony osoby dzielącej się danymi odzwierciedlają zobowiązania umowne osoby dzielącej się danymi wobec pierwotnego posiadacza danych. W przypadku zmiany takich zobowiązań osoby dzielącej się danymi wobec pierwotnego posiadacza danych odbiorca danych zobowiązuje się do przestrzegania wszelkich nowych środków uzgodnionych między osobą dzielącą się danymi a pierwotnym posiadaczem danych.

7. **Prawa własności intelektualnej**

„Prawa własności intelektualnej" oznaczają prawa autorskie (w tym autorskie prawa osobiste i majątkowe), prawa do oprogramowania komputerowego i inne prawa pokrewne), prawa do wzorów (w tym zarejestrowane wzory i prawa ze wzoru), prawa ze znaków towarowych, znaków usługowych, z nazw handlowych, nazw marek, nazw domen i adresów URL, prawa do tajemnic przedsiębiorstwa, *know-how* oraz informacji poufnych i niejawnych (takich jak wynalazki, niezależnie od tego, czy mają zdolność patentową), prawa do logo i patentów, prawa *sui generis* do baz danych oraz wszelkie podobne prawa uznawane na mocy prawa właściwego.

Dane objęte zakresem umowy oraz ich dozwolone wykorzystywanie przez odbiorcę danych muszą być uregulowane w umowie w sposób zapewniający ochronę praw własności intelektualnej osoby dzielącej się danymi, osób trzecich lub nowo powstających praw własności intelektualnej odbiorcy danych. W odniesieniu do kwestii dzielenia się danymi najważniejszymi prawami własności intelektualnej, które należy uwzględnić przy zawieraniu umowy, są prawo *sui generis* przewidziane w dyrektywie w sprawie baz danych oraz prawo autorskie.

Prawo *sui generis*

Zgodnie z art. 43 aktu w sprawie danych „[p]rawo *sui generis* przewidziane w art. 7 dyrektywy 96/9/WE nie ma zastosowania, w przypadku gdy dane są pozyskiwane lub generowane z produktu skomunikowanego lub usługi powiązanej objętych zakresem stosowania niniejszego rozporządzenia, w szczególności w związku z jego art. 4 i 5". Jednakże „[n]ie wpływa to na możliwe stosowanie prawa *sui generis* określonego w art. 7 dyrektywy 96/9/WE względem baz danych zawierających dane niewchodzące w zakres niniejszego rozporządzenia, o ile spełnione są wymagania ochrony zgodnie z ust. 1 tego artykułu" (motyw 112).

Prawo *sui generis* ustanowione dyrektywą w sprawie baz danych chroni producenta bazy danych, ponieważ jest to osoba, która dokonała znaczących inwestycji – pod względem jakościowym lub ilościowym – w celu jej nabycia, weryfikacji lub prezentacji jej zawartości. Producent może zakazać wyodrębniania i wtórnego wykorzystania całości lub istotnej części – ocenianej pod względem jakościowym lub ilościowym – zawartości takiej bazy danych. Poszczególne utwory lub elementy danych w bazie danych, jeżeli są oryginalne, mogą podlegać odrębnej ochronie na podstawie prawa autorskiego, przy czym ochrona ta jest niezależna od ochrony przewidzianej w dyrektywie w sprawie baz danych.

Prawo autorskie

Prawo autorskie jest formą ochrony własności intelektualnej przyznawanej z mocy prawa twórcom oryginalnych utworów autorskich. Ochrona ta obejmuje szeroki zakres utworów, w tym potencjalnie również architekturę bazy danych. Uwaga: ochrona prawnoautorska nie została w pełni zharmonizowana i w związku z tym może się różnić w poszczególnych państwach członkowskich.

Patenty

Dzielenie się danymi oraz wykorzystywanie danych mogą prowadzić do powstania wynalazków, ponieważ sprzyjają generowaniu nowych pomysłów, optymalizacji istniejących technologii oraz przyspieszają rozwój innowacyjnych rozwiązań. Zdolność patentową mają wynalazki o charakterze technicznym, które są nowe i mają poziom wynalazczy oraz mogą być stosowane w przemyśle. Strony powinny zatem uregulować kwestie dotyczące wynalazków i określić, komu przysługuje prawo do korzystania z rezultatów podlegających ochronie patentowej.

7.1. **Wcześniejsze prawa własności intelektualnej**

7.1.1. O ile w umowie wyraźnie nie przewidziano inaczej, każda ze stron zachowuje prawa własności intelektualnej, w tym wszelkie ich zmiany lub ulepszenia, które przysługiwały stronom lub były licencjonowane stronom przez osoby trzecie przed wykonaniem umowy lub całkowicie niezależnie od jej wykonywania („elementy istniejące uprzednio"). W żadnych okolicznościach umowa nie może być uznana za przyznającą którejkolwiek ze stron jakiekolwiek prawo własności intelektualnej do elementów istniejących uprzednio drugiej strony, chyba że umowa wyraźnie stanowi inaczej.

7.1.2. (*jeżeli dane są objęte prawami własności intelektualnej*) Z zastrzeżeniem zapłaty wynagrodzenia (np. opłat licencyjnych) przewidzianego w niniejszej umowie osoba dzieląca się danymi niniejszym udziela odbiorcy danych na czas obowiązywania umowy licencji o następujących cechach: *(określić, np. ogólnoświatowej, niewyłącznej, niezbywalnej)* obejmującej prawo do (*określić, np. wykorzystywania, powielania, modyfikowania, ulepszania, utrzymywania*) danych objętych prawami własności intelektualnej wyłącznie w zakresie niezbędnym do realizacji umowy. Udzielenie sublicencji podwykonawcom odbiorcy danych jest dozwolone wyłącznie do celów podwykonawstwa i w zakresie, w jakim nie jest to niezgodne z postanowieniami niniejszej umowy.

7.2. **Prawa własności intelektualnej do rezultatów**

7.2.1. Jeżeli wykorzystywanie danych przez odbiorcę danych w ramach niniejszej umowy spowoduje powstanie materialnych wytworów pracy, które mogą być chronione prawami własności intelektualnej („rezultaty"), niniejszym uzgadnia się, że:

7.2.2. [WARIANT 1] [odbiorca danych staje się jedynym uprawnionym z tytułu wszelkich praw własności intelektualnej dotyczących rezultatów; jedynie odbiorca danych może, według własnego uznania, dokonać zgłoszenia lub uzyskać jakikolwiek tytuł własności intelektualnej dotyczący rezultatów;

7.2.3. [WARIANT 2] [strony będą wspólnie i na równych zasadach uprawnione z tytułu praw własności intelektualnej do rezultatów oraz zawrą odrębną umowę określającą zasady wykonywania tych praw;

7.2.4. [WARIANT 3] [odbiorca danych zobowiązuje się przenieść, w zakresie niezbędnym, na osobę dzielącą się danymi pełną własność prawną i rzeczywistą oraz wszelkie prawa własności intelektualnej do rezultatów, na zasadzie wyłączności, za rekompensatę, która zostanie uzgodniona między stronami, na cały świat i na cały okres ochrony tych praw własności intelektualnej.

7.2.5. Ponadto strony uzgadniają, że dalsze licencjonowanie rezultatów zostanie przyznane w następujący sposób:

[WARIANT] [(*wskazać stronę, która nie jest uprawniona z tytułu praw własności intelektualnej do rezultatów*) niniejszym udziela (*wskazać stronę, która jest uprawniona z tytułu praw własności intelektualnej do rezultatów*), na okres ochrony praw własności intelektualnej, w pełni płatnej, niewyłącznej i niezbywalnej licencji na cały świat na wykorzystywanie, powielanie, modyfikowanie, ulepszanie oraz utrzymywanie swoich elementów istniejących uprzednio, wyłącznie w zakresie niezbędnym do wykonywania praw do rezultatów na podstawie niniejszej klauzuli.]

[WARIANT] [(*wskazać stronę, która jest uprawniona z tytułu praw własności intelektualnej do rezultatów*) niniejszym udziela (*wskazać stronę, która nie jest uprawniona z tytułu praw własności intelektualnej do rezultatów*), na okres ochrony praw własności intelektualnej, w pełni płatnej, niewyłącznej i niezbywalnej licencji na cały świat na wykorzystywanie, powielanie, modyfikowanie, ulepszanie oraz utrzymywanie rezultatów wyłącznie w następujących celach: (*wypełnić stosownie do przypadku*).]

8. **Wynagrodzenie za zapewnienie dostępu do danych**

Strony mogą, w samej umowie lub w odrębnym dodatku, określić szczegóły dotyczące wynagrodzenia, w tym koszty utworzenia API (wykorzystywanego do dzielenia się danymi) lub inne koszty związane z ułatwianiem dzielenia się danymi, w tym wszelkie honoraria, tantiemy autorskie lub opłaty licencyjne, w zależności od przypadku. Powinny one uzgodnić co najmniej: wysokość należnego wynagrodzenia oraz odpowiednią walutę, termin, w którym wynagrodzenie staje się wymagalne, oraz procedury płatności.

W stosownych przypadkach strony mogą uzgodnić dalsze wynagrodzenie za usługi dodatkowe, które będą podlegać dodatkowej opłacie.

Strony uzgadniają, że odbiorca danych wypłaci wynagrodzenie osobie dzielącej się danymi w następujący sposób: *(wypełnić stosownie do przypadku)*

Powinny one uzgodnić co najmniej: wysokość należnego wynagrodzenia oraz odpowiednią walutę, termin, w którym płatność staje się wymagalna oraz procedury płatności.

9. **Data rozpoczęcia stosowania, okres obowiązywania i rozwiązanie umowy**

9.1. **Data rozpoczęcia stosowania i okres obowiązywania**

9.1.1. Niniejsza umowa [WARIANT 1] [wchodzi w życie ze skutkiem natychmiastowym] [WARIANT 2] [wchodzi w życie z dniem (*wskazać datę*)].

9.1.2. [WARIANT] [Niniejsza umowa zostaje zawarta [WARIANT 1] [na czas nieokreślony] [WARIANT 2] [na czas określony (*wskazać*)], z zastrzeżeniem wszelkich podstaw do jej wygaśnięcia lub rozwiązania przewidzianych w niniejszej umowie.]

9.1.3. [WARIANT] [Osoba dzieląca się danymi musi rozpocząć udostępnianie danych odbiorcy danych [WARIANT 1] bez zbędnej zwłoki po wejściu w życie umowy. [WARIANT 2] w dniu (*wskazać datę oraz – w stosownych przypadkach – dalsze szczegóły dotyczące czasu*).]

Jeżeli wniosek dotyczy jednorazowego dostarczenia danych, wystarczy uzgodnić datę rozpoczęcia stosowania w klauzuli 9.1.1. Jeżeli wniosek dotyczy ciągłego dostarczania danych, strony będą musiały uzgodnić okres obowiązywania umowy oraz wybrać wariant pierwszy albo drugi w klauzuli 9.1.2.

9.2. **Rozwiązanie umowy bez podania przyczyny**

9.2.1. Odbiorca danych może rozwiązać umowę w dowolnym momencie okresu obowiązywania umowy, przekazując osobie dzielącej się danymi wypowiedzenie z zachowaniem okresu *(wskazać okres)*.

9.2.2. [WARIANT] Jeżeli odbiorca danych rozwiąże umowę na podstawie klauzuli 9.3.1 przed (*wskazać moment w czasie lub minimalny okres obowiązywania umowy*), musi wypłacić osobie dzielącej się danymi rekompensatę za koszty poniesione przez osobę dzielącą się danymi w związku z udostępnieniem danych, w tym – w stosownych przypadkach – z zapewnieniem wszelkiego dodatkowego wsparcia, w następujący sposób: *(określić)*.

Mogą wystąpić przypadki, w których osoba dzieląca się danymi ponosi wydatki na udostępnienie danych odbiorcy danych, takie jak dostosowanie swojej infrastruktury cyfrowej, przy założeniu, że wydatki te z czasem się zamortyzują.

W takim przypadku osoba dzieląca się danymi może chcieć zapewnić sobie otrzymanie rekompensaty od odbiorcy danych.

9.3. **Skutki wygaśnięcia lub rozwiązania umowy**

9.3.1. Wygaśnięcie okresu obowiązywania umowy lub rozwiązanie niniejszej umowy zwalnia obie strony z zobowiązania do wykonania oraz do przyjęcia przyszłego świadczenia, lecz nie wpływa na prawa i zobowiązania, które powstały do chwili rozwiązania umowy.

Wygaśnięcie lub rozwiązanie umowy nie ma wpływu na żadne postanowienie niniejszej umowy dotyczące rozstrzygania sporów na podstawie klauzuli 11.6 ani na jakiekolwiek inne postanowienie, które ma obowiązywać również po zakończeniu obowiązywania umowy.

9.3.2. [WARIANT 1] [Przy zakończeniu umowy osoba dzieląca się danymi musi zastosować odpowiednie środki wsparcia odejścia, jakich odbiorca danych może zasadnie oczekiwać.] [WARIANT 2] [Przy zakończeniu umowy osoba dzieląca się danymi musi zastosować następujące środki wsparcia odejścia: (określić).]

Strony mogą rozważyć, czy odbiorca danych wymaga jakichkolwiek środków wsparcia odejścia przy zakończeniu umowy.

Będzie to miało znaczenie na przykład w przypadku, gdy odbiorca danych był uprawniony do wyodrębnienia danych z nośnika lub środowiska kontrolowanego przez osobę dzielącą się danymi, lecz nie wyodrębnił jeszcze tych danych, ponieważ nie spodziewał się rozwiązania umowy.

10. **Środki ochrony prawnej w przypadku naruszenia umowy**

10.1. **Przypadki niewykonania zobowiązania**

10.1.1. Niewykonanie zobowiązania jest istotnym naruszeniem zobowiązania, jeżeli:

a) niewykonanie zobowiązania w znacznym stopniu pozbawia drugą stronę tego, czego miała prawo oczekiwać na podstawie niniejszej umowy, chyba że strona, która nie wykonała zobowiązania, nie przewidziała i nie mogła w rozsądny sposób przewidzieć takiego rezultatu, lub

b) z okoliczności jasno wynika, że nie można polegać na przyszłym wykonaniu zobowiązań przez stronę, która nie wykonała zobowiązania.

10.1.2. Niewykonanie zobowiązania przez stronę jest usprawiedliwione, jeżeli wynika z przeszkody pozostającej poza jej kontrolą oraz jeżeli nie można było w rozsądny sposób oczekiwać, aby w chwili zawarcia niniejszej umowy strona ta uwzględniła tę przeszkodę bądź jej uniknęła lub przezwyciężyła ją lub jej skutki.

Jeżeli przeszkoda jest tylko tymczasowa, niewykonanie zobowiązania przez stronę jest usprawiedliwione tylko w okresie, w którym istnieje przeszkoda. Jeżeli jednak opóźnienie stanowi istotne naruszenie zobowiązania, druga strona może je tak traktować.

Strona, która nie wykonała zobowiązania, ma obowiązek dopilnować, aby zawiadomienie o przeszkodzie oraz jej wpływie na możliwość wykonania zobowiązania dotarło do drugiej strony bez zbędnej zwłoki po tym, jak strona, która nie wykonała zobowiązania, dowiedziała się lub powinna była się dowiedzieć o tych okolicznościach. Druga strona jest uprawniona do odszkodowania za szkodę ekonomiczną wynikłą z nieotrzymania takiego zawiadomienia.

10.2. **Środki ochrony prawnej w przypadku naruszenia**

10.2.1. W przypadku niewykonania zobowiązania przez jedną ze stron drugiej stronie przysługują środki ochrony prawnej wymienione w poniższych klauzulach, bez uszczerbku dla wszelkich środków ochrony prawnej dostępnych na podstawie prawa właściwego.

10.2.2. Dopuszczalne jest łączenie środków ochrony prawnej, które wzajemnie się nie wykluczają.

10.2.3. Strona nie może skorzystać ze środka ochrony prawnej w zakresie, w jakim sama spowodowała niewykonanie zobowiązania przez drugą stronę, na przykład gdy uchybienie w jej własnej infrastrukturze danych uniemożliwiło drugiej stronie należyte wykonanie jej zobowiązań. Strona nie może również powoływać się na roszczenie odszkodowawcze z tytułu poniesionych szkód w zakresie, w jakim mogła ograniczyć powstałą szkodę przez podjęcie zasadnych kroków.

10.2.4. Strona poszkodowana może:

a) rozwiązać niniejszą umowę ze skutkiem natychmiastowym i bez ponoszenia kar, w drodze wypowiedzenia złożonego drugiej stronie, jeżeli:

(i) niewykonanie zobowiązania przez drugą stronę stanowi istotne naruszenie zobowiązania lub

(ii) w przypadku niewykonania, które nie stanowi istotnego naruszenia zobowiązania, strona poszkodowana wezwała drugą stronę do naprawienia naruszenia bez zbędnej zwłoki, a druga strona tego nie uczyniła.

b) dochodzić odszkodowania za szkodę ekonomiczną poniesioną w wyniku niewykonania zobowiązania przez drugą stronę, jeżeli to niewykonanie nie jest usprawiedliwione na mocy klauzuli 10.1.2. Strona, która nie wykonała zobowiązania, ponosi odpowiedzialność wyłącznie za szkodę, którą przewidywała lub którą mogła w rozsądny sposób przewidzieć w chwili zawarcia niniejszej umowy jako prawdopodobny skutek niewykonania zobowiązania, chyba że niewykonanie zobowiązania miało charakter umyślny lub stanowiło rażące zaniedbanie;

c) żądać, aby strona, która nie wykonała zobowiązania, bez zbędnej zwłoki wykonała swoje zobowiązania wynikające z niniejszej umowy, chyba że byłoby to niezgodne z prawem lub niemożliwe lub wykonanie zobowiązania powodowałoby dla strony, która nie wykonała zobowiązania, koszty niewspółmierne do korzyści, jakie uzyskałaby druga strona.

10.2.5. [WARIANT] [W przypadku gdy strona nie wykona swoich zobowiązań wynikających z niniejszej umowy, jest ona w każdym przypadku zobowiązana do zapłaty kar umownych określonych szczegółowo w dodatku 5, które strony uznają za odszkodowanie w rozumieniu klauzuli 10.2.4 lit. b). Stronie, która nie wykonała zobowiązania, przysługuje prawo żądania obniżenia kary do rozsądnej wysokości, jeżeli strona ta wykaże, że kara jest rażąco wygórowana w stosunku do szkody wynikającej z niewykonania zobowiązania.]

11. **Postanowienia ogólne**

11.1. **Poufność**

11.1.1. Następujące informacje muszą być uważane za poufne:

a) informacje odnoszące się do tajemnic przedsiębiorstwa, sytuacji finansowej lub jakiegokolwiek innego aspektu działalności drugiej strony, chyba że dana druga strona sama podała te informacje do publicznej wiadomości;

b) informacje określające podstawę obliczenia zasadnej rekompensaty;

c) informacje dotyczące wszelkich osób trzecich, chyba że informacje te zostały już podane przez nie do wiadomości publicznej.

11.1.2. Obie strony zgadzają się zastosować wszelkie uzasadnione środki w celu bezpiecznego przechowywania oraz zachowania pełnej poufności informacji, o których mowa w klauzuli 11.1.1, oraz nie ujawniać ani nie udostępniać takich informacji osobom trzecim, chyba że:

a) jedna ze stron jest prawnie zobowiązana do ujawnienia lub udostępnienia odpowiednich informacji lub

b) jedna ze stron musi ujawnić lub udostępnić odpowiednie informacje w celu wypełnienia swoich zobowiązań wynikających z niniejszej umowy, lub

c) jedna ze stron uzyskała uprzednią zgodę drugiej strony lub strony, która przekazała informacje poufne lub której ujawnienie tych informacji dotyczy.

11.1.3. Te zobowiązania do zachowania poufności pozostają w mocy po rozwiązaniu niniejszej umowy przez okres (*wskazać okres*).

11.1.4. Te zobowiązania do zachowania poufności nie znoszą ani nie ograniczają bardziej rygorystycznych obowiązków wynikających z (i) rozporządzenia (UE) 2016/679 (RODO), (ii) przepisów wdrażających dyrektywę 2002/58/WE lub dyrektywę (UE) 2016/943 ani (iii) żadnego innego prawa UE ani prawa państwa członkowskiego.

11.2. **Środki komunikacji**

Wszelkie zawiadomienia lub inne komunikaty wymagane lub dozwolone na mocy niniejszej umowy muszą mieć formę pisemną i mogą być doręczane osobiście, wysyłane pocztą przesyłką opłaconą z góry lub przekazywane drogą elektroniczną, w tym pocztą elektroniczną, pod warunkiem że nadawca zachowa dowód wysłania na adresy wskazane poniżej:

Strona	Osoba wyznaczona do kontaktów	E-mail	Telefon	Adres
Użytkownik	[Imię i nazwisko]/[Stanowisko]	[E-mail]	[Telefon]	[Adres]
Odbiorca danych	[Imię i nazwisko]/[Stanowisko]	[E-mail]	[Telefon]	[Adres]

Każde takie zawiadomienie lub każdy taki komunikat uznaje się za otrzymane:

a) w przypadku doręczenia osobistego – w dniu doręczenia,

b) w przypadku wysłania pocztą przesyłką opłaconą z góry – w trzecim dniu roboczym po dniu nadania,

c) w przypadku przekazania drogą elektroniczną – w dniu przekazania, pod warunkiem że nadawca nie otrzymał żadnego komunikatu o błędzie wskazującego na niedoręczenie.

11.3. **Całość umowy, zmiany i rozdzielność postanowień**

11.3.1. Niniejsza umowa (wraz z dodatkami, o których mowa w niniejszej umowie) stanowi całość umowy między stronami w odniesieniu do jej przedmiotu i zastępuje wszelkie wcześniejsze umowy, porozumienia i uzgodnienia stron – zarówno ustne, jak i pisemne – dotyczące przedmiotu niniejszej umowy.

11.3.2. Wszelkie zmiany niniejszej umowy będą ważne wyłącznie wtedy, gdy zostaną uzgodnione przez strony na piśmie, w tym w jakiejkolwiek formie elektronicznej.

11.3.3. Jeżeli którekolwiek postanowienie niniejszej umowy zostanie uznane za nieważne, bezskuteczne, wzruszalne lub niewykonalne z jakiegokolwiek powodu i jeżeli postanowienie to można oddzielić od pozostałych postanowień umowy, te pozostałe postanowienia pozostaną ważne i wykonalne, chyba że danego postanowienia nie można oddzielić od pozostałych postanowień niniejszej umowy. Wszelkie powstałe w ten sposób luki lub niejasności w niniejszej umowie rozstrzyga się zgodnie z klauzulą 11.5.

11.4. **Prawo właściwe**

Niniejsza umowa podlega prawu *(określić państwo członkowskie)*.

11.5. **Interpretacja**

11.5.1. Każde postanowienie niniejszej umowy należy interpretować w sposób zapewniający zgodność z przepisami prawa Unii lub przepisami krajowymi przyjętymi zgodnie z prawem Unii, a także z wszelkimi mającymi zastosowanie przepisami prawa krajowego, które są zgodne z prawem Unii i których nie można wyłączyć w drodze umowy.

11.5.2. Jeżeli jakiejkolwiek luki lub niejasności w niniejszej umowie nie można usunąć w sposób, o którym mowa w klauzuli 11.5.1, umowę tę należy interpretować w świetle zasad wykładni przewidzianych w prawie właściwym (zob. klauzula 11.4).

11.6. **Rozstrzyganie sporów**

11.6.1. Strony uzgadniają, że dołożą wszelkich starań w celu polubownego rozstrzygania sporów i że przed wniesieniem sprawy do sądu przekażą spór do [wstawić nazwę i dane kontaktowe konkretnego organu rozstrzygania sporów].

11.6.2. [WARIANT] [Sądy (*określić państwo członkowskie*) będą miały wyłączną właściwość do rozpoznania sprawy dotyczącej niniejszej umowy.]

Dodatek 1 zawiera opis danych

[do opracowania przez strony]

Dodatek 2 zawiera dalsze szczegółowe informacje dotyczące danych objętych uregulowaniami wymagającymi szczególnych środków

[do opracowania przez strony]

Dodatek 3 zawiera szczegółowe informacje na temat danych osobowych i odnośnych obowiązków stron

[do opracowania przez strony]

Dodatek 4 zawiera środki bezpieczeństwa mające zastosowanie do dzielenia się danymi

[do opracowania przez strony]

[WARIANT] Dodatek 5 zawiera szczegółowe informacje na temat kar

[do opracowania przez strony]

ZAŁĄCZNIK VI

STANDARDOWE POSTANOWIENIA UMOWNE

dotyczące zmiany dostawcy i odejścia klienta

Główne cele rozporządzenia (UE) 2023/2854 (zwanego dalej aktem w sprawie danych) w zakresie zmiany dostawcy w chmurze obejmują umożliwienie klientom usług przetwarzania danych (usług przetwarzania w chmurze oraz usług przetwarzania brzegowego): (i) dokonania zmiany pomiędzy dostawcami oferującymi usługę tego samego typu, (ii) przejścia na lokalną infrastrukturę ICT lub (iii) jednoczesnego korzystania z usług wielu różnych dostawców. W związku z tym w akcie w sprawie danych określono prawa i obowiązki dostawców i klientów w odniesieniu do tego procesu. W tym kontekście klienci powinni również ocenić swoje cele związane ze zmianą dostawcy, a zwłaszcza szczególne potrzeby, dodatkowe wydatki lub kwestie czasowe. Dostawca, klient oraz docelowy dostawca muszą współpracować w dobrej wierze, aby zapewnić skuteczność procesu zmiany dostawcy, umożliwić terminowe przekazanie danych oraz utrzymać ciągłość usług przetwarzania danych (art. 27 aktu w sprawie danych).

Niniejsze standardowe postanowienia umowne przekładają nowe prawa i obowiązki wprowadzone aktem w sprawie danych w odniesieniu do procesu zmiany dostawcy i odejścia klienta na postanowienia umowne. W akcie w sprawie danych zobowiązano dostawców do dostarczenia klientom pisemnej umowy określającej zasady procesu zmiany dostawcy. Umowa musi również określać harmonogram zmiany dostawcy (maksymalny okres przejściowy wynoszący 30 dni) oraz szczegółowe informacje na temat wszelkich związanych z tym kosztów (w tym kar za wcześniejsze rozwiązanie umowy, standardowych opłat za usługę – art. 29 ust. 4 aktu w sprawie danych – oraz opłat z tytułu wychodzącego ruchu danych). Istnieją również obowiązki związane z samym procesem zmiany dostawcy, które należy określić w umowie: zapewnienie uzasadnionej pomocy klientowi (oraz wszelkim osobom trzecim upoważnionym przez klienta), utrzymanie ciągłości działania i zapewnienie wysokiego poziomu bezpieczeństwa w trakcie całego procesu zmiany dostawcy.

Opłaty z tytułu zmiany dostawcy

Zgodnie z art. 29 aktu w sprawie danych dostawca może utrzymać opłaty z tytułu zmiany dostawcy do 12 stycznia 2027 r., ale nie mogą one przekraczać kosztów poniesionych przez dostawcę, które są bezpośrednio związane z procesem zmiany dostawcy. W przypadku zmiany dostawcy dokonywanej po 12 stycznia 2027 r. dostawca nie może nakładać opłat z tytułu zmiany dostawcy. Opłaty z tytułu zmiany dostawcy obejmują opłaty z tytułu wychodzącego ruchu danych oraz inne koszty działań, które dostawca jest zobowiązany przeprowadzić w ramach procesu zmiany dostawcy. Obejmuje to na przykład koszty korzystania z zautomatyzowanych narzędzi do zmiany dostawcy lub narzędzi testowych, jeżeli są one wykorzystywane przez dostawcę do wypełnienia jego obowiązków wynikających z aktu w sprawie danych.

W przypadku równoczesnego korzystania z wielu usług przetwarzania danych dostawcy mogą – nawet po 12 stycznia 2027 r. – nadal przenosić na klienta koszty poniesione z tytułu wychodzącego ruchu danych (art. 34 aktu w sprawie danych).

O ile w akcie w sprawie danych „opłaty z tytułu zmiany dostawcy" zdefiniowano jako opłaty „nakładane przez dostawcę usług przetwarzania danych na klienta za działania wymagane zgodnie z niniejszym rozporządzeniem w celu zmiany na system innego dostawcy lub lokalną infrastrukturę ICT [...]", art. 25 ust. 2 lit. a) pkt (i) aktu w sprawie danych stanowi również, że dostawca „zapewnia klientowi i osobom trzecim upoważnionym przez klienta uzasadnioną pomoc w procesie zmiany dostawcy". Wszelkie opłaty związane ze świadczeniem takiej „uzasadnionej pomocy" powinny być stopniowo wycofywane w sposób wskazany w art. 29 aktu w sprawie danych.

W akcie w sprawie danych określono przypadki, w których zastosowanie podejścia standardowego nie jest możliwe:

— art. 29 ust. 5 „[w] stosownym przypadku dostawcy usług przetwarzania danych przedstawiają klientowi informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi"

— oraz art. 29 ust. 6: „W stosownym przypadku dostawcy usług [...] publicznie przedstawiają informacje [...]".

Do niniejszego dokumentu dołączone są także inne standardowe postanowienia umowne zalecane przez Komisję, obejmujące szczególne zagadnienia inne niż zmiana dostawcy i odejście klienta. Zachęca się strony do rozważenia stosowania również tych pozostałych klauzul, ponieważ zostały opracowane tak, aby były spójne i wzajemnie się uzupełniały.

Szczegółowe uregulowania

Warto zauważyć, że w art. 31 aktu w sprawie danych przewidziano pewne wyjątki od niektórych obowiązków dotyczących zmiany dostawcy i odejścia klienta uwzględnionych w standardowych postanowieniach umownych. Na przykład szczegółowe uregulowania dotyczące niektórych usług przetwarzania danych mają zastosowanie do zmiany dostawcy usług przetwarzania danych w sytuacji, gdy:

(a) większość głównych cech usługi przetwarzania danych została opracowana na zamówienie, aby dostosować je do konkretnych potrzeb indywidualnego klienta, LUB wszystkie komponenty zostały opracowane na potrzeby indywidualnego klienta oraz

(b) te usługi przetwarzania danych nie są oferowane komercyjnie na szeroką skalę w katalogu usług dostawcy, oraz
(c) dostawca należycie poinformował klienta, że obowiązki dotyczące zmiany dostawcy nie mają zastosowania do tej konkretnej usługi.

W zależności od konkretnego wyjątku niektóre obowiązki prawne mogą nie mieć zastosowania. Jednak to do klienta i dostawcy należy uzgodnienie, czy włączyć je do umowy. Mimo że te standardowe postanowienia umowne nie zostały opracowane w celu uwzględnienia takich sytuacji, mogą one nadal służyć jako inspiracja dla stron umowy dotyczącej takich usług.

Dostawca powinien informować przyszłych klientów, na długo przed zawarciem umowy, o konkretnych usługach, do których mają zastosowanie szczegółowe uregulowania określone w art. 31 aktu w sprawie danych.

Nic nie stoi na przeszkodzie, aby dostawca ostatecznie wprowadził takie usługi na dużą skalę, w którym to przypadku musiałby wywiązywać się ze wszystkich obowiązków związanych ze zmianą dostawcy określonych w akcie w sprawie danych.

Podejścia do zmiany dostawcy

Coraz większa liczba dostawców oferuje narzędzia samoobsługowe do zmiany dostawcy, zarówno w odniesieniu do wchodzącego ruchu danych, gdy klienci rozpoczynają korzystanie z usługi, jak i wychodzącego ruchu danych, gdy klienci zaprzestają korzystania z usługi i dokonują zmiany na lokalną infrastrukturę ICT albo na nowego (docelowego) dostawcę. W przypadku niektórych usług przetwarzania danych takie narzędzia mogą nie być dostępne lub mogą nie umożliwiać pełnej zmiany dostawcy.

W tych standardowych postanowieniach umownych przewidziano dwa podejścia do planowania i przeprowadzania procesu zmiany dostawcy:
(a) zmianę dostawcy opartą na planie zmiany dostawcy i odejścia klienta (wariant A) oraz
(b) zmianę dostawcy z wykorzystaniem zautomatyzowanych narzędzi (wariant B).

Warianty te można ze sobą łączyć. Na przykład w **dodatku 1** „Plan zmiany dostawcy i odejścia klienta" strony mogą również przewidzieć wykorzystanie zautomatyzowanych narzędzi, które mogą mieć zastosowanie do niektórych rodzajów usług lub do niektórych danych.

W ramach obu podejść dostawcy są zobowiązani do usunięcia przeszkód utrudniających skuteczną zmianę dostawcy, jak określono w rozporządzeniu (UE) 2023/2854, zgodnie z którym dostawcy przekazują „klientowi informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych" (art. 26 lit. a)); a „[w]yjściowy dostawca usług przetwarzania danych ułatwia proces zmiany dostawcy, zapewniając zasoby, odpowiednie informacje, dokumentację, wsparcie techniczne oraz w stosownym przypadku niezbędne narzędzia" (art. 30).

Należy również zauważyć, że od dostawcy nie oczekuje się dzielenia się danymi ani wykazywania danych specyficznych dla wewnętrznego funkcjonowania usługi przetwarzania danych dostawcy, jeżeli istnieje ryzyko naruszenia tajemnicy przedsiębiorstwa dostawcy. Zgodnie z zobowiązaniami umownymi określonymi w art. 25 ust. 2 lit. f) od dostawcy wymaga się jedynie szczegółowej specyfikacji kategorii takich danych.

Czy standardowe postanowienia umowne mają zastosowanie do wszystkich modeli usług w chmurze (np. do umów IaaS, PaaS lub SaaS)?

Niniejsze standardowe postanowienia umowne mają zastosowanie do wszystkich rodzajów modeli umów dotyczących usług w chmurze, w przypadku gdy dana usługa w chmurze odpowiada definicji usługi przetwarzania danych określonej w art. 2 pkt 8. Zgodnie z tym artykułem „usługa przetwarzania danych" oznacza „świadczoną na rzecz klienta usługę cyfrową umożliwiającą wszechobecny sieciowy dostęp na żądanie do wspólnego zbioru konfigurowalnych, skalowalnych i elastycznych zasobów obliczeniowych o charakterze scentralizowanym, rozproszonym lub wysoce rozproszonym, które mogą być szybko przydzielone i uwolnione przy minimalnym wysiłku pod względem zarządzania lub interakcji z dostawcą usług". Przepisy aktu w sprawie danych mają zatem zastosowanie do rodzajów usług, które wykazują następujące cechy wymienione w definicji usług przetwarzania danych:

— umożliwiają dostęp do zasobów obliczeniowych, w tym sieci, serwerów, pamięci, aplikacji i usług;

— umożliwiają sieciowy dostęp na żądanie, co oznacza, że klient może jednostronnie dostarczać zasoby obliczeniowe, które są dostępne za pośrednictwem sieci i standardowych mechanizmów, na przykład za pośrednictwem telefonów komórkowych, laptopów lub stacji roboczych;

— mogą być szybko przydzielone i uwolnione przy minimalnym wysiłku pod względem zarządzania lub interakcji z dostawcą usług, co oznacza, że jednostronnego dostarczenia można dokonać bez znaczącej interwencji ze strony usługodawcy i szybko je wdrożyć, co umożliwia organizacjom niemal natychmiastowe rozpoczęcie korzystania z zasobów;

— są elastyczne i mogą być szybko przydzielone, co oznacza, że rozwiązania mogą być łatwo skalowane w celu dostosowania do zmieniających się potrzeb oraz że użytkownicy mogą zwiększać lub zmniejszać zapotrzebowanie w zależności od swoich wymagań.

Dostawca, którego oferta usług wykazuje te cechy, musi przestrzegać przepisów aktu w sprawie danych, aby umożliwić zmianę dostawcy usług przetwarzania danych. Obejmuje to na przykład dostosowanie umów o świadczenie usług do art. 25, obniżenie i wycofanie opłat z tytułu zmiany dostawcy oraz opłat z tytułu wychodzącego ruchu danych zgodnie z art. 29, a także przestrzeganie technicznych aspektów zmiany dostawcy określonych w art. 30. Nie wszystkie wymogi nałożone na usługi przetwarzania danych na podstawie rozdziału VI aktu w sprawie danych mają jednak zastosowanie do SaaS. W szczególności pojęcie równoważności funkcjonalnej ustanowione w art. 30 ust. 1 ma zastosowanie wyłącznie do dostawców IaaS, podczas gdy art. 30 ust. 2 i 3 mają zastosowanie do dostawców PaaS i SaaS. Te dwa ostatnie przepisy nakładają na dostawców usług PaaS i SaaS obowiązek udostępniania otwartych interfejsów oraz zapewnienia zgodności z otwartymi specyfikacjami w zakresie interoperacyjności i normami zharmonizowanymi opublikowanymi w unijnym repozytorium.

Art. 30 aktu w sprawie danych wprowadza rozróżnienie między:
1. IaaS zdefiniowanymi jako „usług[i] przetwarzania danych, które to usługi dotyczą skalowalnych i elastycznych zasobów obliczeniowych ograniczonych do elementów infrastruktury, takich jak serwery, sieci i zasoby wirtualne niezbędne do obsługi infrastruktury, ale nie zapewniają dostępu do usług operacyjnych, oprogramowania i aplikacji, które są przechowywane, w inny sposób przetwarzane lub wdrażane na tych elementach infrastruktury”

oraz
2. innymi rodzajami usług w chmurze.

Ponadto w motywie 81 aktu w sprawie danych doprecyzowano, że ogólne pojęcie „usług przetwarzania danych” obejmuje znaczną liczbę usług o bardzo szerokich i różnorodnych celach, funkcjach i konfiguracjach technicznych i powszechnie uznaje się, że należą do co najmniej jednego z trzech modeli świadczenia usług przetwarzania danych, tj. IaaS, PaaS i SaaS.

Zdolności stron

W art. 24 aktu w sprawie danych wyjaśniono, że „[o]bowiązki dostawców usług przetwarzania danych określone w art. 23, 25, 29, 30 i 34 mają zastosowanie wyłącznie do usług, umów lub praktyk handlowych wyjściowego dostawcy usług przetwarzania danych”.

Między innymi znajomość struktury danych oraz relacji pomiędzy danymi jest wymagana do określenia sekwencji operacji służących eksportowi danych eksportowalnych. Poniższy wykaz ma zatem na celu przedstawienie stronom ogólnych wskazówek, które mają ułatwić wzajemne zrozumienie zdolności każdej ze stron leżących u podstaw poszczególnych etapów procesu zmiany dostawcy. Wykaz ten ma jednak jedynie charakter orientacyjny, a między poniższymi kategoriami modeli usług i w ich obrębie występują istotne niuanse, które mogą różnić się w zależności od konkretnej usługi przetwarzania danych. Strony powinny zwrócić szczególną uwagę na takie różnice.

IaaS

— Klient zna określoną przez siebie strukturę bazy danych. Dostawca IaaS nie zna struktury bazy danych. Dostawca IaaS jest w stanie podać szczegółowe informacje dotyczące metod przeniesienia oraz, w stosownych przypadkach, niezbędnych narzędzi.

— Klient jest w stanie określić sekwencję operacji, okno czasowe i wymagane zasoby IT.

— Dostawca jest w stanie potwierdzić dostępność wymaganych zasobów IT w tym oknie czasowym.

— Klient jest w stanie zainicjować zmianę dostawcy w uzgodnionym terminie.

— Klient odpowiada za import danych do środowiska docelowego oraz ich wdrożenie w tym środowisku.

PaaS

— Klient zna określoną przez siebie strukturę bazy danych.

— Dostawca PaaS również zna charakterystykę bazy danych, ponieważ klient zwrócił się do niego o świadczenie usług takich jak przydział przestrzeni, optymalizacja, reorganizacja i tworzenie kopii zapasowych.

— Dostawca PaaS ma praktyczne doświadczenie w zakresie procedur dotyczących operacji takich jak tworzenie kopii zapasowych. Zna on wymagane zasoby i czas, który upłynął od stworzenia poprzedniej kopii zapasowej. Dostawca PaaS jest w stanie podać szczegółowe informacje dotyczące metod przeniesienia oraz, w stosownych przypadkach, niezbędnych narzędzi, a także informacje na temat harmonogramu i wymaganych zasobów IT.

— Klient jest w stanie określić sekwencję operacji, okno czasowe (okres, taki jak weekend, w którym klient zamierza uniemożliwić użytkownikom dostęp do swoich systemów i w którym nie będą dokonywane aktualizacje, tak aby dane zostały zamrożone, a klient mógł dokonać zmiany dostawcy) oraz wymagane zasoby IT.

— Dostawca jest w stanie potwierdzić dostępność wymaganych zasobów IT w tym oknie czasowym.

— Klient inicjuje zmianę dostawcy w uzgodnionym terminie.

SaaS

— Klient nie zna struktury bazy danych.

— Dostawca SaaS zna określoną przez siebie strukturę bazy danych.

— Dostawca SaaS zna procedury i czas potrzebny do przeprowadzenia operacji takich jak tworzenie kopii zapasowych, optymalizacja i reorganizacja.

— W przypadku instalacji nowej wersji oprogramowania SaaS zawierającej nową wersję struktury bazy danych nierzadko dokonuje się pełnego eksportu ze starej struktury, a następnie pełnego importu do nowej struktury. Procedura ta daje dostawcy SaaS praktyczny wgląd w procedurę, zasoby i czas potrzebne do eksportu danych.

— Dostawca SaaS jest w stanie podać szczegółowe informacje dotyczące metod przeniesienia oraz, w stosownych przypadkach, niezbędnych narzędzi,

— a także informacje na temat harmonogramu i wymaganych zasobów IT

— oraz zaproponować metody i formaty eksportu oraz sekwencję operacji.

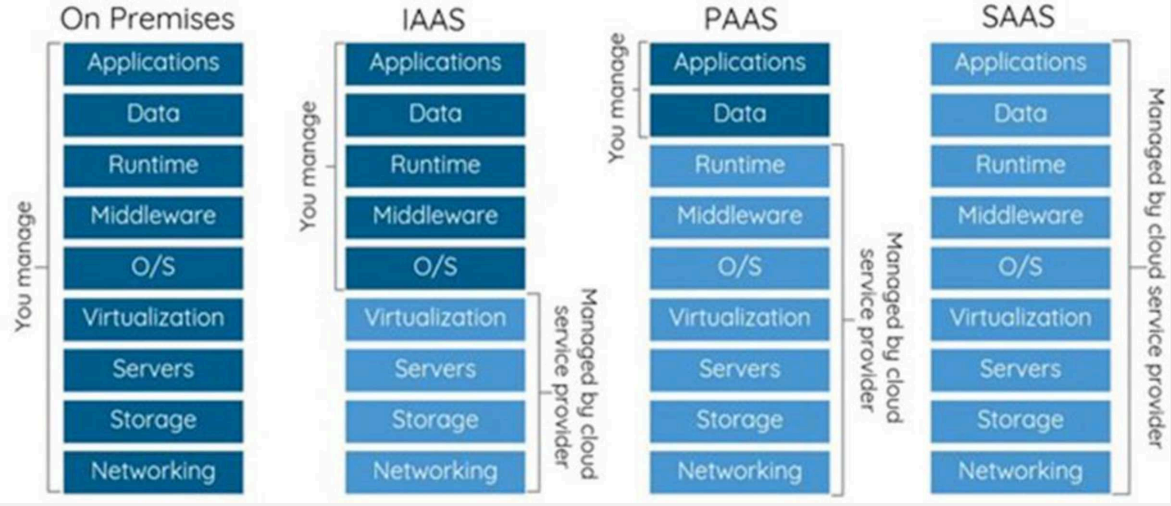
— Klient odpowiada za import danych do środowiska docelowego i może zgłaszać wymagania oraz uwagi dotyczące zaproponowanej sekwencji.

— Dostawca SaaS i klient są w stanie uzgodnić sekwencję operacji, okno czasowe i wymagane zasoby IT.

— Dostawca jest w stanie potwierdzić dostępność wymaganych zasobów IT w tym oknie czasowym.

— W zależności od użytego narzędzia oraz uzgodnionej sekwencji zmianę dostawcy inicjuje dostawca lub klient w uzgodnionym terminie.

— Klient odpowiada za import danych do środowiska docelowego.



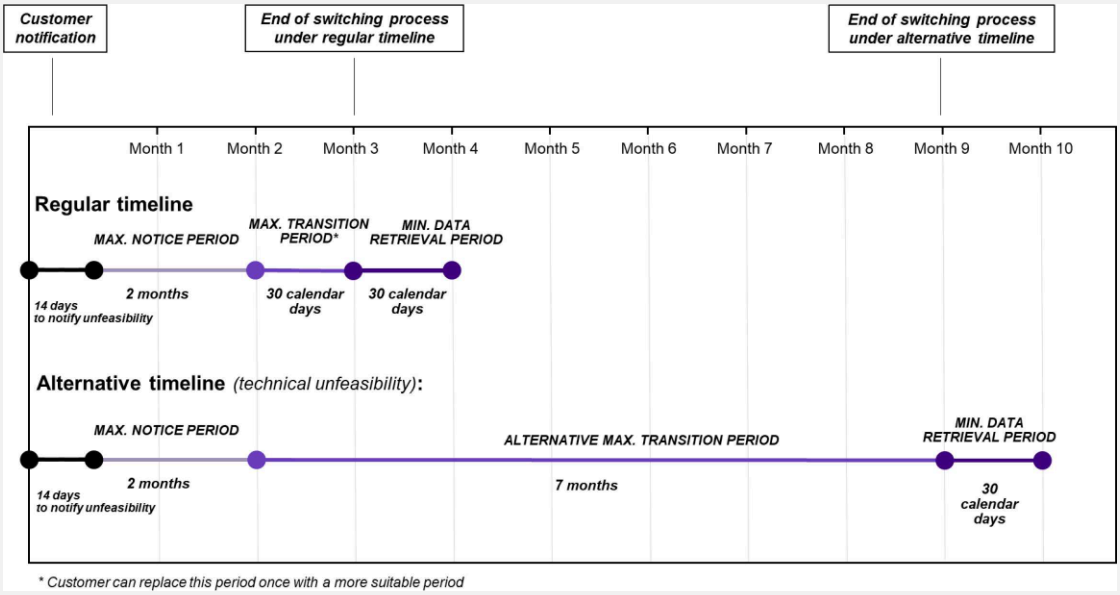
Działania w trakcie maksymalnego okresu wypowiedzenia oraz okresu przejściowego

Rozpoczynanie zmiany dostawcy: w art. 25 ust. 2 lit. d) aktu w sprawie danych wymaga się, aby umowy przewidywały maksymalny okres wypowiedzenia rozpoczynający proces zmiany dostawcy, który nie może przekraczać dwóch miesięcy. W niniejszej klauzuli określono, jakie informacje dostawca powinien przekazać klientowi w tym okresie oraz jakie działania podejmie dostawca po rozpoczęciu procesu zmiany dostawcy.

Okres przejściowy: art. 25 ust. 2 lit. a) aktu w sprawie danych zawiera wymóg, aby umowy zawierały postanowienia umożliwiające klientowi zmianę, na wniosek, na inną usługę przetwarzania danych lub przeniesienie wszystkich danych eksportowalnych do lokalnej infrastruktury ICT bez zbędnej zwłoki i w żadnym razie nie później niż po upływie obowiązkowego maksymalnego okresu przejściowego wynoszącego 30 dni kalendarzowych po zakończeniu maksymalnego okresu wypowiedzenia.

W art. 25 ust. 2 lit. g) aktu w sprawie danych wymaga się również, aby umowa przewidywała minimalny okres, w którym można pobrać dane, wynoszący co najmniej 30 dni kalendarzowych, rozpoczynający się po zakończeniu okresu przejściowego uzgodnionego przez strony.

W przypadku gdy dotrzymanie obowiązkowego maksymalnego okresu przejściowego na zmianę dostawcy, wynoszącego 30 dni, jest technicznie niemożliwe, dostawca musi powiadomić o tym klienta w terminie 14 dni roboczych od złożenia wniosku o zmianę dostawcy, uzasadnić techniczną niewykonalność i wskazać zastępczy okres przejściowy, który nie może przekroczyć siedmiu miesięcy (art. 25 ust. 4 aktu w sprawie danych). Klientowi przysługuje prawo do jednokrotnego przedłużenia obowiązkowego maksymalnego okresu przejściowego o okres, który klient uznaje za bardziej odpowiedni (art. 25 ust. 5 aktu w sprawie danych).



Umowę o przetwarzaniu danych uznaje się za rozwiązaną z chwilą pomyślnego zakończenia zmiany dostawcy lub po upływie maksymalnego okresu wypowiedzenia, jeżeli klient nie zamierza zmienić dostawcy, ale chce skasować swoje dane eksportowalne i aktywa cyfrowe po zakończeniu świadczenia usługi. W takim przypadku złożenie przez klienta wypowiedzenia nie jest konieczne, ponieważ umowa ulega rozwiązaniu automatycznie. W celu zapewnienia pewności prawa oraz ochrony interesów stron dostawca jest jednak zobowiązany zawiadomić klienta o rozwiązaniu umowy (art. 25 ust. 2 lit. c) aktu w sprawie danych).

Wariant A: plan zmiany dostawcy i odejścia klienta jako załącznik do umowy

Przed zawarciem umowy strony mogą rozważyć opracowanie szczegółowego planu zmiany dostawcy i odejścia klienta. Może to być przydatne zwłaszcza w przypadku złożonych usług przetwarzania danych. Przedstawiony tutaj plan zmiany dostawcy i odejścia klienta daje stronom jasną wizję procesu zmiany dostawcy od początku stosunku umownego, w tym w odniesieniu do tego, jakie rodzaje informacji, danych i procesów będą musiały być wymieniane między stronami w celu zmiany dostawcy niezwłocznie i bez wpływu na usługi lub działalność klienta.

Wzór „planu zmiany dostawcy i odejścia klienta" w **dodatku 1** jest jedynie przykładem takiego planu i ma na celu wskazanie klientowi kwestii, o które powinien zapytać dostawcę, oraz zobrazowanie struktury takiej dyskusji.

Podział obowiązków w trakcie procesu zmiany dostawcy jest przykładem dostosowanym, w stosownych przypadkach, do praw i obowiązków zapisanych w akcie w sprawie danych. Z poszanowaniem tych praw i obowiązków strony mogą jednak uzgodnić inny podział lub uwzględnić dodatkowe szczegóły.

Z tego powodu plan nie jest tożsamy ze standardowym postanowieniem umownym. Jednym z rozwiązań jest zachowanie go jako odrębnego technicznego załącznika do umowy, który może być zmieniany lub aktualizowany przez strony niezależnie. Alternatywnie strony mogą chcieć włączyć załącznik do samej umowy.

Załącznik ten może stanowić standardowy plan zmiany dostawcy i odejścia klienta zaproponowany przez dostawcę i zaakceptowany przez klienta lub plan dostosowany do potrzeb klienta zaproponowany przez dostawcę.

Strony mogą aktualizować plan zmiany dostawcy i odejścia klienta w okresie obowiązywania umowy, stosownie do rozwoju usług przetwarzania danych oraz danych objętych umową, w terminach uzgodnionych przez strony. Aktualizacja ta może również wpływać na uzgodniony okres przejściowy, na przykład w granicach określonych w akcie w sprawie danych.

Plan zmiany dostawcy i odejścia klienta ma zastosowanie wyłącznie w przypadku, gdy klient dokonuje zmiany dostawcy lub przechodzi na lokalną infrastrukturę ICT. Nie ma on zastosowania w sytuacji, gdy klient zamierza jedynie doprowadzić do skasowania swoich danych po zakończeniu okresu wypowiedzenia.

Wariant B: samoobsługowe zautomatyzowane narzędzia do zmiany dostawcy

Chociaż korzystanie z samoobsługowych zautomatyzowanych narzędzi do zmiany dostawcy jest powszechne, może wiązać się z pewnymi wyzwaniami. W szczególności problemem może być np. to, że w przypadku usług SaaS niektóre bazy danych oraz ich konfiguracje mogą nie zostać prawidłowo lub w pełni przeniesione, co powoduje konieczność ręcznej interwencji dostawcy. W przypadku gdy dostawca stosuje takie rozwiązanie samoobsługowe, klauzule w wariancie B umożliwiają klientowi zapewnienie, aby umowa zawierała wystarczające informacje na temat procesu i używanego narzędzia. Elementy zawarte w wariancie A (plan zmiany dostawcy i odejścia klienta jako załącznik do umowy) mogą służyć jako źródło inspiracji.

Jeżeli dostawca korzysta z narzędzi do zmiany dostawcy w celu przeprowadzenia działań wymaganych na mocy aktu w sprawie danych w związku z przejściem na system innego dostawcy lub na lokalną infrastrukturę ICT, pobieranie od klienta opłat za korzystanie z tych narzędzi do zmiany dostawcy uznaje się za opłaty z tytułu zmiany dostawcy.

Co w przypadku zmiany dostawcy zakończonej niepowodzeniem? W klauzuli 1.7 wariantu A i w klauzuli 2.6 wariantu B uwzględniono sytuację, w której zmiana dostawcy zakończyła się niepowodzeniem, przez określenie kroków, jakie klient (i jego docelowy dostawca) oraz wyjściowy dostawca muszą podjąć, działając w dobrej wierze, w celu doprowadzenia do pomyślnej zmiany dostawcy lub uruchomienia możliwości kasowania danych, przewidzianej w akcie w sprawie danych.

Przykład: wyjściowy dostawca proponuje rozwiązanie SaaS A, a docelowy dostawca proponuje rozwiązanie SaaS B. Klient zwraca się do wyjściowego dostawcy o pomoc w dokonaniu zmiany dostawcy na docelowego dostawcę przez wyeksportowanie i przekazanie swoich danych eksportowalnych na określony serwer. Mogą wystąpić następujące scenariusze:
1. wyjściowy dostawca nie proponuje skutecznych narzędzi ani procedur umożliwiających wyeksportowanie i przekazanie wszystkich danych eksportowalnych na określony serwer;
2. dane zostały przekazane na określony serwer, jednak klient lub docelowy dostawca nie są w stanie prawidłowo załadować danych.

1. Wariant A: zmiana dostawcy i odejście klienta wraz z planem jako załącznikiem do umowy

1.1. Informacje

1.1.1. Strony potwierdzają, że dostawca udostępnił klientowi w załączniku do umowy lub na swojej stronie internetowej jasne informacje na temat:

a) standardowych opłat za usługę oraz, w stosownych przypadkach, kar za wcześniejsze rozwiązanie umowy,

b) opłat z tytułu zmiany dostawcy,

c) usług, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub – w stosownych przypadkach – z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi,

d) konkretnych usług, w odniesieniu do których obowiązki dotyczące zmiany dostawcy i odejścia klienta nie mają zastosowania – w stosownych przypadkach.

W art. 31 aktu w sprawie danych ustanowiono szczegółowe uregulowania dotyczące niektórych usług przetwarzania danych. W przypadku usług opracowanych na zamówienie lub wysoce zindywidualizowanych niektóre obowiązki w zakresie zmiany dostawcy nie mają zastosowania. Strony muszą uzgodnić sposób możliwego przeprowadzenia takiej zmiany (w tym jej koszt). Obowiązki dotyczące zmiany dostawcy nie mają zastosowania do usług przetwarzania danych świadczonych przez ograniczony okres jako nieprzeznaczona do produkcji wersja do celów testowania i oceny. Mimo że te standardowe postanowienia umowne nie zostały opracowane w celu uwzględnienia takich sytuacji, mogą one nadal służyć jako inspiracja dla stron umowy dotyczącej takich usług.

Zgodnie z art. 30 ust. 6 aktu w sprawie danych od dostawców nie wymaga się opracowania nowych technologii lub usług. Nie są oni również zobowiązani do ujawniania ani przekazywania klientowi lub innemu dostawcy usług przetwarzania danych aktywów cyfrowych, które: (i) są chronione prawami własności intelektualnej, (ii) stanowią tajemnicę przedsiębiorstwa lub (iii) stwarzają zagrożenie dla bezpieczeństwa i integralności usług klienta lub dostawcy.

1.2. **Zmiana dostawcy i odejście klienta**

1.2.1. Korzystając z formularza określonego w dodatku 1, strony uzgadniają „plan zmiany dostawcy i odejścia klienta" (zwany dalej „planem"), który stanowi integralną część umowy i będzie wdrażany przez strony. Plan zawiera:

a) szczegółową specyfikację wszystkich kategorii danych i aktywów cyfrowych, które można przenieść, w tym co najmniej wszystkich danych eksportowalnych (art. 25 ust. 2 lit. e) aktu w sprawie danych),

b) szczegółową specyfikację kategorii danych specyficznych dla wewnętrznego funkcjonowania dostawcy usługi przetwarzania danych, które są wyłączone spośród danych eksportowalnych, w przypadku gdy istnieje ryzyko naruszenia tajemnic przedsiębiorstwa dostawcy (art. 25 ust. 2 lit. f) aktu w sprawie danych),

c) jasne informacje o znanych zagrożeniach dla ciągłości świadczenia funkcji lub usług po stronie wyjściowego dostawcy usług przetwarzania danych (art. 25 ust. 2 lit. a) pkt (iii) aktu w sprawie danych),

d) szczegółowe informacje dotyczące wsparcia w zakresie zmiany dostawcy i odejścia klienta, w tym metod przeniesienia i formatów, a także etapów wymaganych do przeprowadzenia procesu zmiany dostawcy,

e) imię i nazwisko oraz dane kontaktowe przedstawiciela wyznaczonego przez klienta i dostawcę do realizacji planu,

f) szacunkowy czas potrzebny na wyeksportowanie i przekazanie danych oraz aktywów cyfrowych poza środowisko wyjściowego dostawcy,

Wyjściowy dostawca może wspierać proces zmiany dostawcy po stronie klienta, przedstawiając szacunkowy czas niezbędny do wyeksportowania i przekazania danych eksportowalnych poza swoje środowisko, w oparciu o czas wymagany do zaimportowania danych, szacowaną ilość, przepustowość sieci oraz wcześniejsze doświadczenia lub testy. Analogicznie klient może oszacować czas potrzebny na zaimportowanie i wdrożenie danych w środowisku docelowym. Obie strony powinny wykorzystać takie informacje, aby sprawdzić, czy potrzebny jest zastępczy okres przejściowy.

g) limity i ograniczenia techniczne, w tym wynikające z przechowywania danych poza Unią Europejską,

h) opis kolejności operacji związanych ze zmianą dostawcy, zaproponowanej przez dostawcę,

i) opis metody testowania zaproponowanej przez dostawcę, jeżeli przeprowadzane są testy.

1.2.2. Dostawca przekazuje klientowi odniesienie do internetowego rejestru zawierającego struktury i formaty danych, odpowiednie normy oraz otwarte specyfikacje w zakresie interoperacyjności, w których dostępne są dane eksportowalne, pod adresem [*podać link do lokalizacji*] (art. 26 lit. b) aktu w sprawie danych).

1.2.3. Jeżeli klient tego wymaga, dostawca musi udostępnić za pomocą odpowiednich środków elektronicznych informacje wyjaśniające odpowiednie procedury wyznaczonemu personelowi klienta (lub upoważnionym osobom trzecim).

1.2.4. Na wniosek klienta dostawca zorganizuje test albo pomoże klientowi w przeprowadzeniu testu, jak uzgodniono w dodatku 1, w celu sprawdzenia, czy plan działa w praktyce w odniesieniu do danych eksportowalnych i aktywów cyfrowych. Jeżeli podczas testu pojawią się problemy, strony w dobrej wierze przeanalizują przyczyny i uzgodnią rozwiązania.

1.2.5. Dostawca i klient powinni aktualizować plan każdorazowo, gdy jest to konieczne, lub na wniosek klienta, przy czym aktualizacja taka powinna być poparta uzasadnieniem proponowanych zmian.

1.3. **Rozpoczęcie procesu zmiany dostawcy**

1.3.1. Klient rozpoczyna proces zmiany dostawcy, przesyłając dostawcy zawiadomienie o zmianie dostawcy, jak wskazano w klauzuli 1.10, z zachowaniem okresu wypowiedzenia wynoszącego [*strony wskazują uzgodniony okres wypowiedzenia, który nie może przekraczać dwóch miesięcy*]. Jeżeli klient chce zmienić dostawcę wyłącznie w odniesieniu do niektórych usług i odpowiadających im danych lub aktywów cyfrowych, musi to określić w zawiadomieniu o zmianie dostawcy. [WARIANT] [Klient składa zawiadomienie, korzystając z formularza zawartego w **dodatku 3**.]

Z zastrzeżeniem postanowień umowy klient może zdecydować się na zmianę wyłącznie określonego podzbioru usług hostowanych przez wyjściowego dostawcę. W takim przypadku obowiązki związane ze zmianą dostawcy dotyczą wyłącznie takich usług i odpowiadających im danych oraz aktywów cyfrowych; w pozostałych przypadkach zastosowanie nadal mają wcześniej uzgodnione postanowienia umowne.

1.3.2. W zawiadomieniu o zmianie dostawcy klient informuje dostawcę, czy zamierza:

a) zmienić dostawcę usług przetwarzania danych; W takim przypadku klient przekazuje niezbędne szczegółowe informacje dotyczące docelowego dostawcy (art. 25 ust. 3 lit. a) aktu w sprawie danych);

b) przejść na lokalną infrastrukturę ICT klienta (art. 25 ust. 3 lit. b) aktu w sprawie danych) lub

c) nie zmieniać dostawcy, a jedynie skasować swoje dane eksportowalne i aktywa cyfrowe (art. 25 ust. 3 lit. c) aktu w sprawie danych).

d) [WARIANT] [Klient składa zawiadomienie, korzystając z formularza zawartego w **dodatku 4**.]

1.3.3. Dostawca potwierdza klientowi otrzymanie zawiadomienia o zmianie dostawcy nie później niż [w terminie trzech dni roboczych], przy użyciu tego samego środka komunikacji, z którego skorzystał klient.

1.4. **Okres przejściowy**

1.4.1. Klient ma prawo dokonać zmiany dostawcy bez zbędnej zwłoki w ramach maksymalnego okresu przejściowego wynoszącego 30 dni. Klient może uzgodnić z dostawcą okres przejściowy wynoszący (*strony wskazują uzgodniony okres przejściowy, który może wynosić maksymalnie 30 dni kalendarzowych*) (art. 25 ust. 2 lit. a) aktu w sprawie danych).

1.4.2. Jeżeli dostawca nie jest w stanie dotrzymać [obowiązkowego maksymalnego] okresu przejściowego z uwagi na techniczną niewykonalność, dostawca (art. 25 ust. 4 aktu w sprawie danych):

a) zawiadamia klienta w terminie 14 dni roboczych od [daty złożenia zawiadomienia o zmianie dostawcy],

b) wskazuje zastępczy okres przejściowy, który nie może przekraczać siedmiu (7) miesięcy od dnia złożenia przez klienta zawiadomienia o zmianie dostawcy, oraz

c) należycie uzasadnia techniczną niewykonalność.

1.4.3. Klient potwierdza otrzymanie zawiadomienia dotyczącego zastępczego okresu przejściowego [w terminie trzech dni roboczych].

1.4.4. Klient ma prawo do jednokrotnego przedłużenia okresu przejściowego o okres, który uznaje za właściwszy z uwagi na własne cele, nie dłuższy niż [*wskazać liczbę miesięcy*] (art. 25 ust. 5 aktu w sprawie danych). W takim przypadku klient powiadamia dostawcę o swoim zamiarze zgodnie z klauzulą 1.11 przed upływem pierwotnego okresu przejściowego i wskazuje zastępczy okres przejściowy. Dostawca potwierdza otrzymanie takiego zawiadomienia o przedłużeniu [w terminie trzech dni roboczych].

1.4.5. [WARIANT] Klient składa zawiadomienie dotyczące zastępczego okresu przejściowego, korzystając z formularza zawartego w dodatku 5.

1.5. **Obowiązki dostawcy podczas procesu zmiany dostawcy**

1.5.1. Dostawca zobowiązuje się do udzielenia klientowi i osobom trzecim upoważnionym przez klienta uzasadnionej pomocy w procesie zmiany dostawcy od momentu jego rozpoczęcia i przez cały czas jego trwania, tak aby klient mógł zmienić dostawcę w okresie przejściowym. W tym celu dostawca musi w szczególności:

a) zapewnić zdolności, odpowiednie informacje (w tym dokumentację niezbędną do zakończenia procesu zmiany dostawcy) i wsparcie techniczne. W przypadku zidentyfikowania problemów dostawca i klient w dobrej wierze przeanalizują przyczyny i uzgodnią rozwiązania;

b) postępować z należytą starannością w celu utrzymania ciągłości działalności i kontynuować świadczenie funkcji lub usług przewidzianych w umowie (art. 25 ust. 2 lit. a) pkt (ii) aktu w sprawie danych);

c) utrzymywać wysoki poziom bezpieczeństwa w trakcie całego procesu zmiany dostawcy, w szczególności bezpieczeństwa danych podczas ich przekazywania (art. 25 ust. 2 lit. a) pkt (iv) aktu w sprawie danych).

1.6. **Obowiązki klienta podczas procesu zmiany dostawcy**

1.6.1. Klient zobowiązuje się zastosować wszelkie uzasadnione środki, aby dokonać skutecznej zmiany dostawcy. Klient jest odpowiedzialny za import danych i aktywów cyfrowych do swoich własnych systemów lub do systemów docelowego dostawcy oraz za wdrożenie tych danych i aktywów cyfrowych w tych systemach, w tym również w przypadku, gdy klient korzysta w tym celu z usług osoby trzeciej.

1.6.2. W stosownych przypadkach i bez uszczerbku dla art. 30 ust. 6 aktu w sprawie danych klient i dostawca, a także upoważnione przez nich osoby trzecie, zobowiązują się do poszanowania praw własności intelektualnej do wszelkich materiałów dostarczonych przez dostawcę w procesie zmiany dostawcy, jak również tajemnicy przedsiębiorstwa dostawcy. Klient zobowiązuje się zapewnić dostęp do tych materiałów oraz umożliwić ich wykorzystywanie osobom trzecim upoważnionym przez klienta wyłącznie w zakresie niezbędnym do przeprowadzenia procesu zmiany dostawcy oraz wyłącznie po uzyskaniu wyraźnej zgody dostawcy. Dostęp do materiałów dostawcy związanych z procesem zmiany dostawcy, które są chronione prawami własności intelektualnej lub stanowią tajemnice przedsiębiorstwa związane z procesem zmiany dostawcy, a także ich wykorzystywanie, ustaje najpóźniej z końcem uzgodnionego okresu przejściowego, w tym zastępczego okresu przejściowego, w pełnej zgodności ze zobowiązaniami w zakresie poufności i prawami własności intelektualnej przyznanymi przez dostawcę.

1.6.3. Klient działa w dobrej wierze w celu wdrożenia wszelkich wytycznych dotyczących procesu zmiany dostawcy przekazanych przez dostawcę.

1.6.4. Klient może uzgodnić z wyjściowym dostawcą kryteria pomyślnego zakończenia zmiany dostawcy, jak również kamienie milowe procesu zmiany dostawcy, oraz informuje wyjściowego dostawcę o stopniu realizacji tych kamieni milowych podczas procesu zmiany dostawcy. W każdym przypadku klient powinien poinformować dostawcę o pomyślnym zakończeniu zmiany dostawcy.

W uzupełnieniu do zobowiązań wynikających z niniejszej umowy wszystkie zaangażowane strony, w tym docelowi dostawcy usług przetwarzania danych, są zobowiązane na mocy art. 27 aktu w sprawie danych do współpracowania ze sobą w dobrej wierze, aby zapewnić skuteczność procesu zmiany dostawcy, umożliwić terminowe przekazanie danych oraz utrzymać ciągłość usługi przetwarzania danych.

1.7. **Zmiana dostawcy zakończona niepowodzeniem**

1.7.1. Jeżeli proces zmiany dostawcy nie zakończy się pomyślnie, strony muszą współpracować w dobrej wierze w celu zidentyfikowania przyczyn i doprowadzenia do jego pomyślnego zakończenia, umożliwienia terminowego przekazania danych oraz utrzymania ciągłości działania usług. W szczególności, na wniosek klienta, dostawca wspiera klienta w identyfikowaniu przyczyn niepowodzenia zmiany dostawcy, a w zakresie, w jakim zidentyfikowane przyczyny dotyczą środowiska dostawcy lub procesów zmiany dostawcy, doradza, w jaki sposób można rozwiązać zidentyfikowane problemy techniczne. Do wsparcia udzielanego przez dostawcę oraz do innych usług dostawcy, o których mowa w niniejszej sekcji, stosuje się zasady dotyczące opłat z tytułu zmiany dostawcy.

1.7.2. Klient może upoważnić docelowego dostawcę do działania w jego imieniu.

1.8. **Pobieranie i kasowanie danych**

1.8.1. Klient może pobrać lub skasować swoje dane w uzgodnionym okresie pobierania danych, który wynosi […] dni.

1.8.2. Po upływie uzgodnionego okresu pobierania danych i jeżeli pomyślnie zakończono proces zmiany dostawcy, dostawca kasuje wszystkie dane eksportowalne i aktywa cyfrowe wygenerowane przez klienta lub bezpośrednio z nim związane. Dostawca potwierdza [w ciągu x dni roboczych], że zakończył takie kasowanie, z wyjątkiem eksportowalnych danych osobowych, które dostawca jest zobowiązany przechowywać na mocy przepisów unijnych lub krajowych.

Okres pobierania danych rozpoczyna się po zakończeniu uzgodnionego okresu przejściowego i musi trwać co najmniej 30 dni kalendarzowych po zakończeniu okresu przejściowego uzgodnionego między klientem a dostawcą. Klient może zdecydować, że nie skorzysta z przysługującego mu prawa do pobrania danych. W takim przypadku sam skasuje dane (i może poinformować o tym dostawcę, jak określono w art. 25 ust. 3 lit. c) aktu w sprawie danych) albo dostawca skasuje takie niepobrane dane, jak określono w klauzuli 1.8.2 wariantu A i w klauzuli 2.7.2 wariantu B.

1.9. **Opłaty z tytułu zmiany dostawcy**

1.9.1. Opłaty należne od klienta z tytułu zmiany dostawcy są następujące […]

W przypadku równoczesnego korzystania z kilku usług przetwarzania danych (scenariusz wdrożenia wielochmurowego) opłat z tytułu wychodzącego ruchu danych nie uznaje się za opłaty z tytułu zmiany dostawcy i w związku z tym można je nałożyć na klienta w celu przeniesienia takich kosztów poniesionych przez dostawcę, pod warunkiem że nie przekraczają one kosztów rzeczywiście poniesionych. W każdym innym przypadku po 12 stycznia 2027 r. nie można nałożyć na klienta żadnych opłat z tytułu zmiany dostawcy (zob. wyjaśnienia dotyczące opłat z tytułu zmiany dostawcy zawarte w informacji wprowadzającej do niniejszego standardowego postanowienia umownego).

1.10. **Zakończenie procesu zmiany dostawcy**

[Zob. standardowe postanowienia umowne dotyczące rozwiązania umowy]

1.11. **Zawiadomienia**

Strony uzgadniają, że wszelkie zawiadomienia między nimi dotyczące zmiany dostawcy i odejścia klienta będą dokonywane (*strony wskazują wybrane środki komunikacji, z uwzględnieniem odpowiednich środków elektronicznych*).

1.12. **Pierwszeństwo**

W przypadku jakiejkolwiek sprzeczności lub niespójności między niniejszymi klauzulami dotyczącymi zmiany dostawcy i odejścia klienta a innymi mającymi zastosowanie ustaleniami umownymi, postanowieniami, warunkami lub innymi umowami odnoszącymi się do zmiany dostawcy usługi przetwarzania danych pierwszeństwo mają niniejsze klauzule.

2. **Wariant B: Zmiana dostawcy i odejście klienta z wykorzystaniem samoobsługowych zautomatyzowanych narzędzi do zmiany dostawcy**

2.1. **Informacje**

2.1.1. Przed złożeniem zamówienia na usługi przetwarzania danych dostawca przekazał klientowi jasne informacje na temat:

a) dostępnych samoobsługowych zautomatyzowanych narzędzi do zmiany dostawcy takich usług („narzędzia do zmiany dostawcy") oraz warunków ich stosowania,

b) standardowych opłat za usługę oraz, w stosownych przypadkach, kar za wcześniejsze rozwiązanie umowy,

c) opłat z tytułu zmiany dostawcy, w tym opłat za korzystanie z narzędzi do zmiany dostawcy.

W art. 31 aktu w sprawie danych ustanowiono szczegółowe uregulowania dotyczące niektórych usług przetwarzania danych. W przypadku usług opracowanych na zamówienie lub wysoce zindywidualizowanych niektóre obowiązki w zakresie zmiany dostawcy nie mają zastosowania. Strony muszą uzgodnić sposób możliwego przeprowadzenia takiej zmiany (w tym jej koszt). Obowiązki dotyczące zmiany dostawcy nie mają zastosowania do usług przetwarzania danych świadczonych przez ograniczony okres jako nieprzeznaczona do produkcji wersja do celów testowania i oceny. Mimo że te standardowe postanowienia umowne nie zostały opracowane w celu uwzględnienia takich sytuacji, mogą one nadal służyć jako inspiracja dla stron umowy dotyczącej takich usług.

Zgodnie z art. 30 ust. 6 aktu w sprawie danych od dostawców nie wymaga się opracowania nowych technologii lub usług. Nie są oni również zobowiązani do ujawniania ani przekazywania klientowi lub innemu dostawcy usług przetwarzania danych aktywów cyfrowych, które: (i) są chronione prawami własności intelektualnej, (ii) stanowią tajemnicę przedsiębiorstwa lub (iii) stwarzają zagrożenie dla bezpieczeństwa i integralności usług klienta lub dostawcy.

2.1.2. Lista kontrolna dotycząca zmiany dostawcy zawarta w **dodatku 2**, który stanowi integralną część umowy, obejmuje:

a) szczegółową specyfikację wszystkich kategorii danych i aktywów cyfrowych, które można przenieść z wykorzystaniem narzędzi do zmiany dostawcy, w tym co najmniej wszystkich danych eksportowalnych (art. 25 ust. 2 lit. e) aktu w sprawie danych),

b) szczegółową specyfikację kategorii danych specyficznych dla wewnętrznego funkcjonowania dostawcy usługi przetwarzania danych, które są wyłączone spośród danych eksportowalnych, w przypadku gdy istnieje ryzyko naruszenia tajemnic przedsiębiorstwa dostawcy (art. 25 ust. 2 lit. f) aktu w sprawie danych),

c) informacje na temat procedur zmiany dostawcy i przeniesienia usługi z wykorzystaniem narzędzi do zmiany dostawcy, w tym metod i formatów, limitów i ograniczeń technicznych (w tym wynikających z przechowywania danych poza UE), procedur, dokumentacji, a także – w stosownych przypadkach – najlepszych praktyk, zdolności oraz wsparcia technicznego, które dostawca udostępni klientowi (w szczególności podczas testów, przygotowań do zmiany dostawcy oraz samej zmiany dostawcy), w tym wszelkich infolinii dostępnych klientom w trakcie zmiany dostawcy lub alternatywnych kanałów komunikacji oraz scenariuszy testowych; informacje te muszą wyjaśniać, w jaki sposób przenieść wszystkie dane eksportowalne i aktywa cyfrowe w sposób spójny i konsekwentny na tyle szybko, aby umożliwić skuteczną zmianę dostawcy,

d) szacunkowy czas potrzebny na wyeksportowanie i przekazanie danych oraz aktywów cyfrowych poza środowisko wyjściowego dostawcy, w przypadku gdy narzędzia do zmiany dostawcy są wykorzystywane zgodnie z dokumentacją dostawcy,

e) jasne informacje o znanych zagrożeniach dla ciągłości świadczenia funkcji lub usług po stronie wyjściowego dostawcy usług przetwarzania danych (art. 25 ust. 2 lit. a) pkt (iii) aktu w sprawie danych),

f) zasoby, w tym zasoby IT (takie jak serwery, CPU, pamięć, wejścia/wyjścia, szerokość pasma), które dostawca zapewni w celu umożliwienia skutecznej zmiany dostawcy, oraz procedurę uzyskiwania dodatkowych zasobów IT.

2.1.3. Dostawca przekazuje klientowi odniesienie do internetowego rejestru zawierającego struktury i formaty danych, odpowiednie normy oraz otwarte specyfikacje w zakresie interoperacyjności, w których dostępne są dane eksportowalne, pod adresem [*podać link do lokalizacji*] (art. 26 lit. b) aktu w sprawie danych).

2.2. **Rozpoczęcie procesu zmiany dostawcy**

2.2.1. Klient rozpoczyna proces zmiany dostawcy, przesyłając dostawcy zawiadomienie o zmianie dostawcy, jak uzgodniono w klauzuli 2.10, z zachowaniem okresu wypowiedzenia wynoszącego [*strony wskazują uzgodniony okres wypowiedzenia, który nie może przekraczać dwóch miesięcy*]. Jeżeli klient chce zmienić dostawcę wyłącznie w odniesieniu do niektórych usług i odpowiadających im danych lub aktywów cyfrowych, musi to określić w zawiadomieniu o zmianie dostawcy. [WARIANT] [Klient składa zawiadomienie, korzystając z formularza zawartego w **dodatku 3**.]

Zawiadomienie o zmianie dostawcy jest innym instrumentem niż wypowiedzenie umowy. Z zastrzeżeniem postanowień umowy klient może zdecydować się na zmianę wyłącznie określonego podzbioru usług świadczonych przez wyjściowego dostawcę. W takim przypadku obowiązki związane ze zmianą dostawcy dotyczą wyłącznie takich usług i odpowiadających im danych oraz aktywów cyfrowych; w pozostałych przypadkach zastosowanie nadal mają wcześniej uzgodnione postanowienia umowne.

2.2.2. W zawiadomieniu o zmianie dostawcy klient informuje dostawcę, czy zamierza:

a) zmienić dostawcę usług przetwarzania danych; w takim przypadku klient powinien przekazać niezbędne szczegółowe informacje dotyczące docelowego dostawcy;

b) przejść na lokalną infrastrukturę ICT klienta lub

c) nie zmieniać dostawcy, a jedynie skasować swoje dane eksportowalne i aktywa cyfrowe.

d) [WARIANT] [Klient składa zawiadomienie, korzystając z formularza zawartego w **dodatku 4**.]

2.2.3. Klient może również wskazać w zawiadomieniu o zmianie dostawcy okna czasowe na przeprowadzenie zmiany dostawcy oraz dodatkowe zasoby IT wymagane przez klienta w tych oknach czasowych. Jeżeli dostawca nie jest w stanie zapewnić takich zasobów IT we wskazanych oknach czasowych, powinien zgłosić sprzeciw nie później niż [w terminie trzech dni roboczych] od otrzymania zawiadomienia o zmianie dostawcy, przedstawiając należyte uzasadnienie oraz proponując klientowi kilka alternatywnych „okien czasowych", z poszanowaniem maksymalnego okresu przejściowego.

Okna czasowe na zmianę dostawcy to okres, na przykład weekend, w którym klient zamierza uniemożliwić użytkownikom dostęp do swoich systemów i w którym nie będą dokonywane aktualizacje, tak aby dane zostały zamrożone, a klient mógł dokonać zmiany dostawcy.

2.2.4. Dostawca potwierdza klientowi otrzymanie zawiadomienia o zmianie dostawcy [w terminie trzech dni roboczych], przy użyciu tego samego środka komunikacji, z którego skorzystał klient.

Klient może potrzebować przeprowadzić zmianę dostawcy w określonych ramach czasowych, aby zminimalizować zakłócenie działalności gospodarczej. Ponadto zmiana dostawcy może wymagać dodatkowych zasobów po stronie wyjściowego dostawcy. W związku z tym, w razie potrzeby, klient powinien wskazać okna czasowe, w których zamierza przeprowadzić zmianę dostawcy, oraz dodatkowe zasoby (zgodnie z informacjami przekazanymi przez wyjściowego dostawcę). Jeżeli wyjściowy dostawca nie jest w stanie zapewnić takich zasobów w tych oknach czasowych z uzasadnionych powodów (np. zaplanowane prace utrzymaniowe usług, które istotnie wpływałyby na dostępność zasobów w tym czasie), powinien zaproponować klientowi alternatywne rozwiązania, które zapewnią skuteczną zmianę dostawcy przed upływem maksymalnego okresu przejściowego.

2.3. **Okres przejściowy**

2.3.1. Jeżeli dostawca nie jest w stanie dotrzymać [obowiązkowego maksymalnego] okresu przejściowego z uwagi na techniczną niewykonalność, dostawca zobowiązuje się:

a) zawiadomić klienta na piśmie, w tym za pomocą odpowiednich środków elektronicznych, w terminie 14 dni roboczych od [daty złożenia zawiadomienia o zmianie dostawcy],

b) wskazać zastępczy okres przejściowy, który nie może przekraczać siedmiu (7) miesięcy od dnia złożenia przez klienta zawiadomienia o zmianie dostawcy, oraz

c) należycie uzasadnić techniczną niewykonalność.

Klient potwierdza otrzymanie takiego zawiadomienia o przedłużeniu [w terminie trzech dni roboczych].

2.3.2. Klient ma prawo do jednokrotnego przedłużenia okresu przejściowego o okres, który uznaje za właściwszy z uwagi na własne cele, nie dłuższy niż [*wskazać liczbę miesięcy*]. W takim przypadku klient powiadamia dostawcę o swoim zamiarze na piśmie, w tym za pomocą odpowiednich środków elektronicznych, przed upływem pierwotnego okresu przejściowego i wskazuje zastępczy okres przejściowy. Dostawca potwierdza otrzymanie takiego zawiadomienia o przedłużeniu [w terminie trzech dni roboczych].

[WARIANT] [Klient składa zawiadomienie, korzystając z formularza zawartego w **dodatku 5**.]

2.4. **Obowiązki dostawcy podczas procesu zmiany dostawcy**

2.4.1. Dostawca zobowiązuje się do udzielenia klientowi i osobom trzecim upoważnionym przez klienta uzasadnionej pomocy w procesie zmiany dostawcy od momentu jego rozpoczęcia i przez cały czas jego trwania, tak aby klient mógł zmienić dostawcę w okresie przejściowym. W tym celu dostawca musi w szczególności:

a) postępować z należytą starannością w celu utrzymania ciągłości działalności i kontynuować świadczenie funkcji lub usług przewidzianych w umowie;

b) utrzymywać wysoki poziom bezpieczeństwa w trakcie całego procesu zmiany dostawcy, w szczególności bezpieczeństwa danych podczas ich przekazywania, oraz

c) jeżeli w trakcie zmiany dostawcy zostaną wykryte problemy, których nie można rozwiązać w ramach wsparcia technicznego, wspólnie z klientem przeanalizować ich przyczyny i uzgodnić rozwiązania.

Nawet w wariancie B („samoobsługowe zautomatyzowane narzędzia do zmiany dostawcy") dostawca ponosi współodpowiedzialność za harmonogram zmiany dostawcy, na przykład w sytuacji, gdy narzędzia te działają zbyt wolno, aby zapewnić pomyślne zakończenie procesu zmiany dostawcy, lub jeżeli dostawca reaguje z nieuzasadnionym opóźnieniem, gdy klient wykryje problem wymagający wsparcia dostawcy.

2.5. **Obowiązki klienta podczas procesu zmiany dostawcy**

2.5.1. Klient zobowiązuje się zastosować wszelkie uzasadnione środki, aby dokonać skutecznej zmiany dostawcy. Klient przyjmuje na siebie odpowiedzialność za import danych i aktywów cyfrowych do swoich własnych systemów lub do systemów docelowego dostawcy oraz za wdrożenie tych danych i aktywów cyfrowych, w tym również w przypadku, gdy klient korzysta w tym celu z usług osoby trzeciej.

2.5.2. W stosownych przypadkach i bez uszczerbku dla art. 30 ust. 6 aktu w sprawie danych klient i dostawca, a także upoważnione przez nich osoby trzecie, zobowiązują się do poszanowania praw własności intelektualnej do wszelkich materiałów dostarczonych przez dostawcę w procesie zmiany dostawcy, jak również tajemnicy przedsiębiorstwa dostawcy. Klient zobowiązuje się zapewnić dostęp do tych materiałów oraz umożliwić ich wykorzystywanie osobom trzecim upoważnionym przez klienta wyłącznie w zakresie niezbędnym do przeprowadzenia procesu zmiany dostawcy oraz wyłącznie po uzyskaniu wyraźnej zgody dostawcy. Dostęp do materiałów dostawcy związanych z procesem zmiany dostawcy, które są chronione prawami własności intelektualnej lub stanowią tajemnice przedsiębiorstwa związane z procesem zmiany dostawcy, a także ich wykorzystywanie, ustaje najpóźniej z końcem uzgodnionego okresu przejściowego, w tym zastępczego okresu przejściowego, w pełnej zgodności ze zobowiązaniami w zakresie poufności i prawami własności intelektualnej przyznanymi przez dostawcę.

2.5.3. Klient może uzgodnić z wyjściowym dostawcą kryteria pomyślnego zakończenia zmiany dostawcy, jak również kamienie milowe procesu zmiany dostawcy, oraz informuje wyjściowego dostawcę o stopniu realizacji tych kamieni milowych podczas procesu zmiany dostawcy. W każdym przypadku klient powinien poinformować dostawcę o pomyślnym zakończeniu zmiany dostawcy.

2.5.4. Klient działa w dobrej wierze w celu wdrożenia wszelkich wytycznych dotyczących procesu zmiany dostawcy przekazanych przez dostawcę.

W uzupełnieniu do zobowiązań wynikających z niniejszej umowy wszystkie zaangażowane strony, w tym docelowi dostawcy usług przetwarzania danych, są zobowiązane na mocy art. 27 aktu w sprawie danych do współpracowania ze sobą w dobrej wierze, aby zapewnić skuteczność procesu zmiany dostawcy, umożliwić terminowe przekazanie danych oraz utrzymać ciągłość usługi przetwarzania danych.

Uzasadnione środki stosowane przez klienta w celu zapewnienia skutecznej zmiany dostawcy obejmują w szczególności:

— wewnętrzne przygotowanie procesu zmiany dostawcy (np. wstrzymanie wszelkiego dostępu do danych i poinformowanie użytkownika o niedostępności systemu; w przypadku powierzenia zmiany dostawcy osobie trzeciej – przekazanie takiej osobie trzeciej odpowiednich instrukcji, tak aby przestrzegała umowy zawartej między klientem a dostawcą;

— monitorowanie procesu zmiany dostawcy (np. sprawdzanie eksportowanych danych i aktywów cyfrowych w trakcie zmiany dostawcy w celu natychmiastowego zidentyfikowania wszelkich problemów);

— zawarcie odpowiednich ustaleń umownych z docelowym dostawcą lub zapewnienie odpowiednich zasobów na potrzeby przejścia na infrastrukturę lokalną.

2.6. **Zmiana dostawcy zakończona niepowodzeniem**

2.6.1. Jeżeli proces zmiany dostawcy nie zakończy się pomyślnie, strony muszą współpracować w dobrej wierze w celu zidentyfikowania przyczyn i doprowadzenia do jego pomyślnego zakończenia, umożliwienia terminowego przekazania danych oraz utrzymania ciągłości działania usług. W szczególności, na wniosek klienta, dostawca wspiera klienta w identyfikowaniu przyczyn niepowodzenia zmiany dostawcy, a w zakresie, w jakim zidentyfikowane przyczyny dotyczą środowiska dostawcy lub procesów zmiany dostawcy, doradza, w jaki sposób można rozwiązać zidentyfikowane problemy techniczne. Do wsparcia udzielanego przez dostawcę oraz do innych usług dostawcy, o których mowa w niniejszej sekcji, stosuje się zasady dotyczące opłat z tytułu zmiany dostawcy.

2.6.2. Klient może upoważnić docelowego dostawcę do działania w jego imieniu.

2.7. **Pobieranie i kasowanie danych**

2.7.1. Strony uzgadniają, że klient pobiera lub kasuje swoje dane w uzgodnionym okresie pobierania danych, który wynosi […] dni.

2.7.2. Po upływie uzgodnionego okresu pobierania danych i jeżeli pomyślnie zakończono proces zmiany dostawcy, dostawca zobowiązuje się skasować wszystkie dane eksportowalne i aktywa cyfrowe wygenerowane przez klienta lub bezpośrednio z nim związane oraz potwierdzić klientowi, że je skasował, z wyjątkiem tych danych eksportowalnych, które dostawca jest zobowiązany przechowywać na mocy bezwzględnie obowiązujących przepisów prawa Unii lub prawa państw członkowskich Unii, pod warunkiem że dostawca – jeżeli zezwala na to prawo – poinformuje klienta, które dane eksportowalne zostaną zatrzymane, przez jaki okres oraz na jakiej podstawie.

Okres pobierania danych rozpoczyna się po zakończeniu uzgodnionego okresu przejściowego i musi trwać co najmniej 30 dni kalendarzowych po zakończeniu okresu przejściowego uzgodnionego między klientem a dostawcą. Klient może zdecydować, że nie skorzysta z przysługującego mu prawa do pobrania danych. W takim przypadku sam skasuje dane (i może poinformować o tym dostawcę, jak określono w art. 25 ust. 3 lit. c) aktu w sprawie danych) albo dostawca skasuje takie niepobrane dane, jak określono w klauzuli 1.8 wariantu A i klauzuli 2.7 wariantu B.

2.8. **Opłaty z tytułu zmiany dostawcy**

Opłaty należne od klienta z tytułu zmiany dostawcy są następujące […]

W przypadku równoczesnego korzystania z kilku usług przetwarzania danych (scenariusz wdrożenia wielochmurowego) opłat z tytułu wychodzącego ruchu danych nie uznaje się za opłaty z tytułu zmiany dostawcy i w związku z tym można je nałożyć na klienta w celu przeniesienia takich kosztów poniesionych przez dostawcę, pod warunkiem że nie przekraczają one kosztów rzeczywiście poniesionych. Narzędzia testowe służące do zmiany dostawcy oraz uzasadnione wsparcie udzielane klientowi w ramach testowania, zgodnie z planem zmiany dostawcy i odejścia klienta, należy uznawać za część procesu zmiany dostawcy, w związku z czym opłaty za takie usługi powinny być stopniowo wycofywane zgodnie z art. 29 aktu w sprawie danych.

2.9. **Zakończenie procesu zmiany dostawcy**

Zob. klauzula 1 w standardowych postanowieniach umownych dotyczących rozwiązania umowy.

2.10. **Zawiadomienia**

Strony uzgadniają, że wszelkie zawiadomienia między nimi dotyczące zmiany dostawcy i odejścia klienta będą dokonywane [*strony wskazują wybrane środki komunikacji, z uwzględnieniem odpowiednich środków elektronicznych*].

2.11. **Pierwszeństwo**

W przypadku jakiejkolwiek sprzeczności lub niespójności między niniejszymi klauzulami dotyczącymi zmiany dostawcy i odejścia klienta a innymi mającymi zastosowanie ustaleniami umownymi, postanowieniami, warunkami lub innymi umowami odnoszącymi się do zmiany dostawcy usługi przetwarzania danych pierwszeństwo mają niniejsze klauzule.

Dodatek 1

Plan zmiany dostawcy i odejścia klienta

1. **Dane kontaktowe**

a) Dane kontaktowe dostawcy do celów zmiany dostawcy i odejścia klienta: …

b) Dane kontaktowe klienta do celów zmiany dostawcy i odejścia klienta: …

2. **Klient musi podać w pisemnym zawiadomieniu następujące informacje:**

a) dane objęte zawiadomieniem, zgodnie z uzgodnioną identyfikacją w **dodatku 2**,

b) docelowe miejsce przekazania danych: lokalna infrastruktura ICT klienta lub docelowy dostawca, wraz z odpowiednimi specyfikacjami technicznymi dotyczącymi miejsca docelowego,

c) lokalizację, do której dane powinny zostać wyeksportowane i dostarczone.

3. **Obowiązki dostawcy w zakresie reakcji na pisemne zawiadomienie**

W terminie …. dni dostawca udzieli klientowi pisemnej odpowiedzi zawierającej następujące informacje:

a) szczegółową specyfikację wszystkich kategorii danych, które mają zostać przekazane podczas procesu zmiany dostawcy, w tym:

(i) dane eksportowalne

— wszystkie dane zaimportowane przez klienta na początku obowiązywania umowy o świadczenie usług, w tym metadane (dane wejściowe):

— A, z metadanymi: ….. w formacie ….

— B, z metadanymi: ….. w formacie ….

— C, z metadanymi: ….. w formacie ….

— wszystkie dane bezpośrednio lub pośrednio współwygenerowane w wyniku korzystania przez klienta z usługi przetwarzania danych:

— D, z metadanymi: ….. w formacie ….

— E, z metadanymi: ….. w formacie ….

— F, z metadanymi: ….. w formacie ….

(ii) aktywa cyfrowe

— L, w formacie …

— M, w formacie …

b) szczegółową specyfikację kategorii danych specyficznych dla wewnętrznego funkcjonowania dostawcy usługi przetwarzania danych, które są wyłączone spośród danych eksportowalnych, w przypadku gdy istnieje ryzyko naruszenia tajemnic przedsiębiorstwa dostawcy: ...

4. **Potwierdzenie danych objętych zmianą dostawcy**

Klient wskaże, które dane i aktywa cyfrowe chce otrzymać w uzgodnionym (lub zastępczym) okresie przejściowym.

5. **Kolejność, harmonogram i testowanie**

W okresie przejściowym:

a) uzgodniona kolejność i harmonogram eksportu oraz przenoszenia wybranych danych i aktywów cyfrowych są następujące: …

b) opis metody testowania zaproponowanej przez dostawcę: ....

c) dostawca lub klient, korzystając z narzędzi do zmiany dostawcy oraz procesów dostawcy, przeprowadza test eksportu i przekazania do uzgodnionej lokalizacji z wykorzystaniem części uzgodnionych danych i aktywów cyfrowych, w celu potwierdzenia lub dostosowania kolejności i harmonogramu;

d) klient testuje import oraz wdrożenie uzgodnionych danych i aktywów cyfrowych we własnych systemach lub w systemach docelowego dostawcy;

e) jeżeli w trakcie testów lub w ich wynikach wystąpią problemy, wyjściowy dostawca i klient ustalają, czy wynikają one z eksportu uzgodnionych danych i aktywów cyfrowych oraz procesów przekazania pozostających w zakresie odpowiedzialności dostawcy, czy też z procesów ich importu i wdrożenia pozostających w zakresie odpowiedzialności klienta.

6. **Realizacja procesu zmiany dostawcy**

a) Dostawca jest zobowiązany wyeksportować i przenieść dane lub aktywa cyfrowe za pomocą środków elektronicznych lub fizycznych do lokalizacji wskazanej przez klienta, a klient (lub osoby trzecie upoważnione przez klienta) jest zobowiązany zaimportować dane lub aktywa cyfrowe do swoich własnych systemów lub do systemów docelowego dostawcy i wdrożyć te dane lub aktywa cyfrowe w ramach tych systemów.

b) Klient (lub osoby trzecie upoważnione przez klienta) jest zobowiązany przetestować funkcje w swoim środowisku lub w środowisku docelowego dostawcy w terminie ... *[strony wskazują uzgodniony termin przeprowadzenia testu]* i udokumentować dostawcy wszelkie problemy wynikające z (i) jakości wyeksportowanych danych lub aktywów cyfrowych lub (ii) niewystarczających informacji przekazanych przez dostawcę.

c) Dostawca jest zobowiązany zareagować bez zbędnej zwłoki, tak aby klient mógł zmienić dostawcę w obowiązkowym okresie przejściowym.

7. **Zmiana dostawcy zakończona pomyślnie**

Gdy tylko klient zawiadomi dostawcę o pomyślnym zakończeniu procesu zmiany dostawcy, dostawca zobowiązuje się bez zbędnej zwłoki zawiadomić klienta o rozwiązaniu umowy. Jeżeli klient nie zawiadomi dostawcy o pomyślnym zakończeniu procesu zmiany dostawcy ani o zmianie dostawcy zakończonej niepowodzeniem, a dostawca ma podstawy, aby sądzić, że klient z powodzeniem zakończył proces zmiany dostawcy, dostawca może zwrócić się do klienta z wnioskiem o potwierdzenie, czy pomyślne zakończenie procesu zmiany dostawcy miało miejsce. Jeżeli klient nie potwierdzi pomyślnego zakończenia procesu zmiany dostawcy w terminie 30 dni kalendarzowych od otrzymania takiego wniosku, uznaje się, że zmiana dostawcy zakończyła się niepowodzeniem, a umowa nie ulega rozwiązaniu.

Dodatek 2

Lista kontrolna dotycząca zmiany dostawcy

Wymagane informacje są wyraźnie wymienione poniżej albo można je znaleźć pod adresem […].

a) Szczegółowa specyfikacja wszystkich kategorii danych i aktywów cyfrowych, które można przenieść, w tym co najmniej wszystkich danych eksportowalnych: ...

b) Szczegółowa specyfikacja kategorii danych i aktywów cyfrowych specyficznych dla wewnętrznego funkcjonowania dostawcy usługi przetwarzania danych, które są wyłączone z procesu zmiany dostawcy, w przypadku gdy istnieje ryzyko naruszenia tajemnic przedsiębiorstwa dostawcy: ...

c) Informacje na temat procedur zmiany dostawcy i przeniesienia usługi z wykorzystaniem narzędzi do zmiany dostawcy: ...

d) Szacunkowy czas potrzebny na wyeksportowanie i przekazanie danych oraz aktywów cyfrowych: ...

e) Znane zagrożenia dla ciągłości świadczenia funkcji lub usług po stronie wyjściowego dostawcy: …

f) Zasoby IT, które dostawca zapewni w celu skutecznej zmiany dostawcy: ...

Dodatek 3

Zawiadomienie o zmianie dostawcy

[imię i nazwisko/nazwa i adres dostawcy do celów komunikacji]

[data]

Zawiadomienie o zmianie dostawcy

Imię i nazwisko/nazwa klienta: […]

Umowa: (*nazwa i informacje szczegółowe dotyczące umowy, np. nazwa umowy, jej numer, data zawarcia, zgodnie z wymogami umowy)*

Usługi objęte zmianą dostawcy: [*wszystkie usługi objęte umową*] lub [*wskazać konkretne usługi lub aktywa cyfrowe objęte zmianą dostawcy, jeżeli zmiana dostawcy ma dotyczyć wyłącznie części usług*]

[WARIANT] [Działając w imieniu klienta, informuję/informujemy, że klient inicjuje zmianę dostawcy w odniesieniu do usług objętych zmianą dostawcy od dnia (*wskazać datę rozpoczęcia*). Okres wypowiedzenia wynosi (*określa klient: maksymalnie dwa miesiące; może być krótszy, jeżeli klient tak postanowi*.]

[WARIANT] Działając w imieniu klienta, informuję/informujemy, że klient inicjuje zmianę dostawcy w odniesieniu do następujących usług, danych lub aktywów cyfrowych: …

[WARIANT] Klient informuje, że zamierza dokonać zmiany dostawcy na [*dane nowego dostawcy/lokalnej infrastruktury ICT klienta*].

[WARIANT] [(*dotyczy zautomatyzowanej zmiany dostawcy*) Klient chciałby dokonać zmiany dostawcy w następujących oknach czasowych: (*wskazać daty i szczegółowe informacje*). Klient zwraca się o udostępnienie następujących zasobów IT w tych oknach czasowych (*do uzupełnienia przez klienta*).]

Dane kontaktowe osoby odpowiedzialnej za zmianę dostawcy: (*dane przedstawiciela klienta odpowiedzialnego za proces zmiany dostawcy*).

_____

[podpis upoważnionego przedstawiciela klienta]

Dodatek 4

Zawiadomienie o odejściu klienta

Poniższy formularz ma zastosowanie, jeżeli klient nie chce zmienić dostawcy, a jedynie skasować swoje dane eksportowalne lub aktywa cyfrowe w ramach zarówno wariantu A, jak i wariantu B.

[imię i nazwisko/nazwa i adres dostawcy do celów komunikacji]

[data]

Zawiadomienie o odejściu klienta

Imię i nazwisko/nazwa klienta: […]

Umowa: [*nazwa i informacje szczegółowe dotyczące umowy, np. nazwa umowy, jej numer, data zawarcia, zgodnie z wymogami umowy]*

Skasowane dane/aktywa cyfrowe: [*wszystkie objęte umową*] lub [*wskazać konkretne dane lub aktywa cyfrowe podlegające kasowaniu danych*]

[WARIANT] [Działając w imieniu klienta, informuję/informujemy, że klient inicjuje zmianę dostawcy polegającą wyłącznie na kasowaniu danych/aktywów cyfrowych od dnia (*wskazać datę rozpoczęcia*). Okres wypowiedzenia wynosi (*określa klient: maksymalnie dwa miesiące; może być krótszy, jeżeli klient tak postanowi*)].

[WARIANT] [Dane kontaktowe osoby odpowiedzialnej za zmianę dostawcy: (*dane przedstawiciela klienta odpowiedzialnego za proces zmiany dostawcy*).]

_____

[podpis upoważnionego przedstawiciela klienta]

Dodatek 5

Zawiadomienie o zastępczym okresie przejściowym

[imię i nazwisko/nazwa i adres dostawcy do celów komunikacji]

[data]

Zawiadomienie o zastępczym okresie przejściowym

Imię i nazwisko/nazwa klienta: […]

Umowa: [*nazwa i informacje szczegółowe dotyczące umowy, np. nazwa umowy, jej numer, data zawarcia, zgodnie z wymogami umowy*]

Skasowane dane/aktywa cyfrowe: [*wszystkie objęte umową*] lub [*wskazać konkretne dane lub aktywa cyfrowe podlegające kasowaniu danych*]

[WARIANT] [Działając w imieniu klienta, informuję/informujemy, że klient chce przedłużyć okres przejściowy do dnia nie późniejszego niż (*wskazać datę*)].

[WARIANT] [Dane kontaktowe osoby odpowiedzialnej za zmianę dostawcy: (*dane przedstawiciela klienta odpowiedzialnego za proces zmiany dostawcy*).]

_____

[podpis upoważnionego przedstawiciela klienta]

ZAŁĄCZNIK VII

STANDARDOWE POSTANOWIENIA UMOWNE

dotyczące rozwiązania umowy

Rozporządzenie (UE) 2023/2854 (zwane dalej aktem w sprawie danych) umożliwia klientom usług przetwarzania danych (tj. usług przetwarzania w chmurze i usług przetwarzania brzegowego) zmianę dostawcy lub przeniesienie danych do własnej lokalnej infrastruktury ICT. Dokonanie zmiany dostawcy ma wpływ na to, czy umowa między stronami będzie nadal obowiązywać, czy też ulegnie rozwiązaniu.

Poniższe standardowe postanowienia umowne regulują rozwiązanie umowy pomiędzy klientem a dostawcą w odniesieniu do konkretnej usługi w kontekście zmiany dostawcy. Obejmują one proces rozwiązania umowy o świadczenie usługi. Postanowienia te są bezpośrednio związane ze standardowymi postanowieniami umownymi dotyczącymi zmiany dostawcy i odejścia klienta i przewidują różne możliwości rozwiązania umowy oraz związane z nimi warunki. Umowę o przetwarzanie danych zazwyczaj rozwiązuje się (w całości lub w części) z chwilą pomyślnego zakończenia procesu zmiany dostawcy lub w przypadku, gdy klient nie chce zmienić dostawcy, ale żąda skasowania wszystkich danych, a takie skasowanie danych zakończyło się powodzeniem. W tych standardowych postanowieniach umownych uwzględniono pewne dodatkowe warianty, aby pomóc stronom w scenariuszach nieobjętych aktem w sprawie danych.

Umowa z dostawcą może obejmować kilka usług. Jeżeli niniejsze standardowe postanowienia umowne zostaną włączone do umowy, a następnie klient dokona zmiany dostawcy na docelowego dostawcę wyłącznie w odniesieniu do jednej usługi, podczas gdy pozostałe usługi pozostaną u wyjściowego dostawcy, umowa ulega rozwiązaniu wyłącznie w odniesieniu do tej konkretnej usługi, o ile strony nie uzgodnią inaczej.

Oprócz rozwiązania umowy w związku ze zmianą dostawcy uregulowanego w niniejszych standardowych postanowieniach umownych umowę można również rozwiązać z innych powodów określonych w umowie głównej lub przewidzianych w prawie właściwym. Jeżeli klient naruszy swoje zobowiązania, dostawca może podjąć decyzję o rozwiązaniu umowy i złożyć wypowiedzenie. W takim przypadku klient może przekazać zawiadomienie o zmianie dostawcy, w wyniku czego umowa zostanie przedłużona do czasu pomyślnego zakończenia procesu zmiany dostawcy.

Do niniejszego dokumentu dołączone są także inne standardowe postanowienia umowne zalecane przez Komisję, obejmujące szczególne zagadnienia inne niż rozwiązanie umowy. Zachęca się strony do rozważenia stosowania również tych pozostałych klauzul, ponieważ zostały opracowane tak, aby były spójne i wzajemnie się uzupełniały.

Co obejmują standardowe postanowienia umowne dotyczące rozwiązania umowy?

Scenariusze przewidziane w akcie w sprawie danych: Umowa ulega rozwiązaniu w określonych okolicznościach po pomyślnym zakończeniu procesu zmiany dostawcy (*zdarzenie A*) lub w przypadku, gdy klient nie chce zmienić dostawcy, lecz żąda skasowania wszystkich danych, a takie skasowanie danych zakończyło się powodzeniem (*zdarzenie B*). Umowę uznaje się za rozwiązaną z chwilą pomyślnego zakończenia procesu zmiany dostawcy (*zdarzenie A*) lub po upływie maksymalnego okresu wypowiedzenia (*zdarzenie B*). Nie ma potrzeby składania wypowiedzenia umowy ani przeprowadzenia procedury rozwiązania umowy przewidzianej w umowie, ponieważ umowa ulega rozwiązaniu automatycznie. Dostawca jest jednak zobowiązany zawiadomić klienta, że umowę uznaje się za rozwiązaną (art. 25 ust. 2 lit. c) aktu w sprawie danych). Zawiadomienie to ma charakter wyłącznie informacyjny, ponieważ umowa uległa rozwiązaniu już wcześniej. W związku z tym, nawet jeżeli dostawca opóźni przekazanie takiego zawiadomienia, nie może pobierać żadnych opłat na podstawie rozwiązanej umowy.

Klient powinien jednak poinformować dostawcę o pomyślnym zakończeniu procesu zmiany dostawcy, ponieważ dostawca może o nim nie wiedzieć. Jeżeli dostawca ma powody, aby podejrzewać, że klient dokonał już pomyślnego zakończenia procesu zmiany dostawcy (na przykład klient nie loguje się do usługi lub nie przechowuje żadnych danych w ramach usługi), dostawca może skontaktować się z klientem i zażądać potwierdzenia pomyślnego zakończenia procesu zmiany dostawcy. W przypadku braku odpowiedzi ze strony klienta uznaje się, że zmiana dostawcy zakończyła się niepowodzeniem, a umowa nadal obowiązuje (tj. nie ulega rozwiązaniu) na dotychczasowych warunkach.

W akcie w sprawie danych nie zdefiniowano, czym jest pomyślnie zakończona zmiana dostawcy. Zasadniczo to do klienta należy decyzja, czy zmiana dostawcy zakończyła się pomyślnie. Sam Klient lub klient i dostawca mogą jednak postanowić o ustanowieniu pewnych kryteriów służących ocenie, czy nastąpiło pomyślne zakończenie procesu zmiany dostawcy, w szczególności takich jak:

a) zakończenie przekazywania danych, tj. czy wszystkie dane eksportowalne oraz – w stosownych przypadkach – aktywa cyfrowe zostały przeniesione do środowiska docelowego dostawcy, a także czy zachowano ich prawidłowość, integralność i kompletność; zgodność danych eksportowalnych i aktywów cyfrowych z pierwotnymi danymi i aktywami cyfrowymi, bez jakiejkolwiek utraty lub jakiegokolwiek uszkodzenia;

b) wdrożenie aktywów cyfrowych (w stosownych przypadkach); jeżeli zmiana dostawcy obejmowała przeniesienie aktywów cyfrowych, takich jak własne lub licencjonowane aplikacje klienta, klient powinien sprawdzić, czy takie aktywa cyfrowe zostały zainstalowane, skonfigurowane i działają w środowisku docelowego dostawcy;
c) testowanie nowej usługi: na tym etapie klient powinien sprawdzić, czy usługi oferowane przez docelowego dostawcę działają zgodnie z założeniami przed dokonaniem zmiany dostawcy; w szczególności klient powinien przeprowadzić testy wydajnościowe, funkcjonalne i operacyjne usługi docelowego dostawcy, w tym testy obejmujące przeniesione dane lub aktywa cyfrowe, w celu oceny, czy spełniono kryteria weryfikacji zmiany dostawcy.

W przypadku umowy na czas określony zmiana dostawcy może zakończyć się przed wygaśnięciem umowy lub po jej wygaśnięciu (w tym drugim przypadku zob. zdarzenie D). Jeżeli zmiana dostawcy zakończy się przed wygaśnięciem umowy, umowa wygasa wraz z zakończeniem procesu zmiany dostawcy. W takim przypadku mogą być należne kary za wcześniejsze rozwiązanie umowy (art. 23 lit. a), art. 25 ust. 2 lit. c) i art. 29 ust. 4 aktu w sprawie danych).

Co w przypadku zmiany dostawcy zakończonej niepowodzeniem?

Zob. standardowe postanowienia umowne dotyczące zmiany dostawcy i odejścia klienta.

W celu rozwiązania sytuacji, w której zmiana dostawcy zakończyła się niepowodzeniem, a umowy nie można rozwiązać, strony mogą złożyć skargę do właściwego organu na podstawie aktu w sprawie danych, aby organ ten podjął decyzję. Należy jednak rozumieć, że strony mogą również skorzystać z wszelkich środków prawnych dostępnych w ich jurysdykcji (np. złożyć pozew, wystąpić o nakaz sądowy do sądu cywilnego itp.).

Dwa dodatkowe scenariusze: klauzule 1.4 i 1.5 są opcjonalne i przedstawiają dwa dodatkowe scenariusze do rozważenia przez strony. Chociaż nie wspomniano o nich wyraźnie w akcie w sprawie danych, mogą one wystąpić w praktyce i uwzględniono je w klauzulach w celu ułatwienia stronom rozwiązania takich sytuacji. Scenariusze te są następujące:

— Klient chce przedłużyć okres dostępności swoich danych u wyjściowego dostawcy lub utrzymać umowę z wyjściowym dostawcą, korzystając z opcji zakupu nowej usługi na dłuższy okres, niezależnie od tego, czy jest to poprzedzone zmianą dostawcy usługi, czy też zwykłym rozwiązaniem umowy o świadczenie usługi bez dokonywania zmiany dostawcy. Klient może potrzebować od wyjściowego dostawcy jedynie usługi o ograniczonej funkcjonalności, tj. zapewniającej dostępność jego danych przez dłuższy okres lub utrzymania umowy, tak aby możliwe było zamówienie nowej usługi (*zdarzenie C*).

W takim przypadku, ponieważ dane będą dostępne za pośrednictwem usługi o ograniczonej funkcjonalności, wyjściowy dostawca i klient powinni zawrzeć nową umowę dotyczącą tej dodatkowej usługi lub zmienić obowiązującą umowę (zob. klauzula 1.4.2). W szczególności strony powinny uzgodnić nowy okres pobierania danych. W przypadku umów ramowych klient może chcieć utrzymać stosunek umowny z wyjściowym dostawcą, aby móc szybko kupować nowe usługi bez przechodzenia przez proces zawierania nowej umowy, który w większych organizacjach może być długotrwały i skomplikowany.

Przykład zdarzenia C: klient skutecznie wyeksportował i przekazał swoje dane od wyjściowego dostawcy do docelowego dostawcy, w którego środowisku dane pomyślnie wdrożono; Innym przykładem może być sytuacja, w której klient decyduje się rozwiązać umowę z wyjściowym dostawcą bez późniejszej migracji do innego dostawcy. W obu tych przypadkach klient nie chce jednak, aby jego dane zostały skasowane, lecz woli, aby były one bezpiecznie przechowywane u wyjściowego dostawcy przez okres wykraczający poza uzgodniony okres pobierania danych. Taka dodatkowa usługa udostępniona przez wyjściowego dostawcę nie uniemożliwia rozwiązania pierwotnej umowy, a świadczenie tej usługi odbywa się na podstawie nowej lub zmienionej umowy.

— Umowa na czas określony wygasa przed rozpoczęciem lub zakończeniem procesu zmiany dostawcy (zdarzenie D)

Przykład zdarzenia D: przykładem takiej sytuacji może być przypadek, w którym klient nie złoży zawiadomienia o zmianie dostawcy z wystarczającym wyprzedzeniem. W takim przypadku dane nie zostają przekazane docelowemu dostawcy w dniu, w którym umowa z wyjściowym dostawcą wygasa.

Strony powinny mieć świadomość, że podczas procesu zmiany dostawcy może nastąpić zawieszenie świadczenia usług. W takim przypadku zastosowanie ma ogólna klauzula dotycząca zawieszenia usług zawarta w umowie.
Istnieją również wyłączenia w odniesieniu do niektórych usług opracowanych na zamówienie. Zob. wyjaśnienie towarzyszące standardowym postanowieniom umownym dotyczącym zmiany dostawcy i odejścia klienta.

1. **Rozwiązanie umowy**

1.1. **Proces rozwiązania umowy**

1.1.1. Umowa zostanie uznana za rozwiązaną między stronami w przypadku wystąpienia jednego z następujących zdarzeń:

a) w stosownych przypadkach, z chwilą pomyślnego zakończenia procesu zmiany dostawcy. Jeżeli pomyślne zakończenie procesu zmiany dostawcy nastąpi przed upływem uzgodnionego okresu obowiązywania umowy, zastosowanie mają opłaty z tytułu wcześniejszego rozwiązania umowy określone w niniejszej umowie; lub

b) na zakończenie maksymalnego okresu wypowiedzenia, w przypadku gdy klient nie chce zmienić dostawcy, ale chce usunąć wszystkie swoje dane eksportowalne i aktywa cyfrowe po zakończeniu usługi;

1.1.2. jeżeli umowa zawiera jakiekolwiek postanowienia dotyczące rozwiązania, z zastrzeżeniem prawa właściwego, takie jak wymienione poniżej:

a) strona wystąpiła o zawieszenie płatności lub została postawiona w stan upadłości,

b) strona nie wykonała w odpowiednim terminie zobowiązania wynikającego z umowy, co skutkuje lub może skutkować rozwiązaniem umowy (na podstawie umowy albo z mocy prawa),

c) nastąpiła zmiana własności lub kontroli strony, która skutkuje lub może skutkować rozwiązaniem umowy – na podstawie umowy lub z mocy prawa

d) umowę uznano za nieważną z powodu naruszenia lub zmiany przepisów bezwzględnie obowiązujących lub

e) wystąpiły inne okoliczności, które skutkują lub mogą skutkować rozwiązaniem umowy – na podstawie umowy lub z mocy prawa;

nawet jeżeli podczas procesu zmiany dostawcy wystąpi którakolwiek z przesłanek rozwiązania umowy, umowa oraz uzgodnione usługi i funkcje nie ulegają rozwiązaniu ani nie wygasają przed pomyślnym zakończeniem procesu zmiany dostawcy (zob. klauzula 1.1.1 lit. a), ani po upływie maksymalnego okresu wypowiedzenia, w przypadku gdy klient zamierza wyłącznie skasować swoje dane eksportowalne i aktywa cyfrowe z chwilą zakończenia usługi (zob. klauzula 1.1.1 lit. b), o ile bezwzględnie obowiązujące przepisy prawa nie stanowią inaczej. Nie ma to wpływu na żadne inne prawa ani środki ochrony prawnej przysługujące stronie wobec drugiej strony. Ma to również zastosowanie w przypadku, gdy proces zmiany dostawcy rozpocznie się po tym, jak dostawca złożył wypowiedzenie umowy.

1.1.3. Bez uszczerbku dla innych środków ochrony prawnej dostępnych na mocy prawa właściwego umowa nie ulega rozwiązaniu ani nie wygasa przed pomyślnym zakończeniem procesu zmiany dostawcy, wydaniem stosownej decyzji przez właściwy sąd lub zawarciem porozumienia między stronami.

1.2. **Rozwiązanie umowy po zakończeniu zmiany dostawcy**

1.2.1. Umowa nie ulega rozwiązaniu do czasu pomyślnego zakończenia procesu zmiany dostawcy. Gdy tylko klient zawiadomi dostawcę o pomyślnym zakończeniu procesu zmiany dostawcy, dostawca bez zbędnej zwłoki zawiadamia klienta o rozwiązaniu umowy.

1.2.2. Jeżeli klient nie zawiadomi dostawcy o pomyślnym zakończeniu procesu zmiany dostawcy ani o zmianie dostawcy zakończonej niepowodzeniem, a dostawca ma uzasadnione podstawy, aby sądzić, że klient z powodzeniem zakończył proces zmiany dostawcy, dostawca może zwrócić się do klienta z wnioskiem o potwierdzenie, czy pomyślne zakończenie procesu zmiany dostawcy miało miejsce. Jeżeli klient nie potwierdzi pomyślnego zakończenia procesu zmiany dostawcy w terminie 30 dni roboczych od otrzymania takiego wniosku, uznaje się, że zmiana dostawcy zakończyła się niepowodzeniem, a umowa nie ulega rozwiązaniu i obowiązuje nadal na dotychczasowych warunkach.

1.3. **Rozwiązanie umowy bez zmiany dostawcy**

1.3.1. Jeżeli klient nie chce zmienić dostawcy, ale chce usunąć swoje dane eksportowalne i aktywa cyfrowe po zakończeniu usługi, jak określono w klauzuli 1.1.1 lit. b), może to nastąpić i zostanie uznane za zakończone tylko wtedy, gdy:

a) upłynął [maksymalny] uzgodniony okres wypowiedzenia oraz

b) klient wyraźnie zwrócił się do dostawcy o skasowanie danych, a w odpowiedzi dostawca pomyślnie skasował dane i potwierdził ten fakt,

c) na zakończenie uzgodnionego okresu wypowiedzenia dostawca powiadomił klienta o rozwiązaniu umowy.

Inne scenariusze [klauzule opcjonalne do rozważenia]

1.4. **Przedłużone zatrzymywanie danych**

1.4.1. Pod koniec okresu przejściowego klient może podjąć decyzję o nieskasowaniu wszystkich swoich danych eksportowalnych i aktywów cyfrowych po upływie [minimalnego]/uzgodnionego okresu pobierania danych oraz o zapewnieniu ich dostępności, w tym do celów świadczenia usługi o ograniczonej funkcjonalności, przez określony, przedłużony okres.

1.4.2. W takim przypadku klient i dostawca uzgadniają (i) zmianę obowiązującej umowy w celu uwzględnienia przedłużonego okresu pobierania danych albo (ii) zawarcie nowej umowy dotyczącej usługi o ograniczonej funkcjonalności.

1.5. **Wygaśnięcie umowy na czas określony przed zmianą dostawcy**

1.5.1. Jeżeli umowa została zawarta na czas określony oraz (i) data jej wygaśnięcia przypada przed zakończeniem procesu zmiany dostawcy oraz (ii) klient nie zażądał skasowania swoich danych eksportowalnych i aktywów cyfrowych, wówczas:

a) okres przejściowy rozpoczyna się z dniem wygaśnięcia umowy; dostawca zapewnia uzasadnioną pomoc zgodnie ze standardowymi postanowieniami umownymi dotyczącymi zmiany dostawcy i odejścia klienta;

b) po pomyślnym zakończeniu procesu zmiany dostawcy zastosowanie ma klauzula 1.2 oraz

c) w przypadku zmiany dostawcy zakończonej niepowodzeniem zastosowanie mają postanowienia standardowych postanowień umownych dotyczących zmiany dostawcy i odejścia klienta: wariant A klauzuli 1.7 lub wariant B klauzuli 2.6.

1.6. **Zawiadomienia**

Strony uzgadniają, że wszelkie zawiadomienia między nimi w odniesieniu do klauzul dotyczących rozwiązania umowy będą dokonywane [*strony wskazują wybrane środki komunikacji, z uwzględnieniem odpowiednich środków elektronicznych*].

1.7. **Pierwszeństwo**

W przypadku jakiejkolwiek sprzeczności lub niespójności między niniejszymi klauzulami dotyczącymi rozwiązania umowy a innymi mającymi zastosowanie ustaleniami umownymi, postanowieniami, warunkami lub innymi umowami odnoszącymi się do rozwiązania umowy stanowiącej podstawę świadczenia usług przetwarzania danych, pierwszeństwo mają niniejsze klauzule.

ZAŁĄCZNIK VIII

STANDARDOWE POSTANOWIENIA UMOWNE

dotyczące bezpieczeństwa i ciągłości działania

Motyw 94 rozporządzenia (UE) 2023/285 (zwanego dalej „aktem w sprawie danych") stanowi, że podczas całego procesu zmiany dostawcy należy zachować wysoki poziom bezpieczeństwa oraz że dostawca powinien postępować z należytą starannością w celu utrzymania ciągłości działalności i zapewnić świadczenie funkcji lub usług przewidzianych w umowie, a także przedstawiać jasne informacje o znanych zagrożeniach dla ciągłości działania.

W akcie w sprawie danych określono obowiązki dostawcy w zakresie zapewnienia wysokiego poziomu bezpieczeństwa i ciągłości działania w związku z procesem zmiany dostawcy. W szczególności dotyczy to bezpieczeństwa danych podczas ich przekazywania i dalszego bezpieczeństwa danych podczas okresu zatrzymywania (art. 25 ust. 2 lit. a) pkt (iv) aktu w sprawie danych). Chociaż kwestie bezpieczeństwa i ciągłości działania są zasadniczo uwzględnione w umowie o przetwarzaniu danych oraz w innej dokumentacji umownej, niniejsze standardowe postanowienia umowne koncentrują się na bezpieczeństwie i ciągłości działania w kontekście procesu zmiany dostawcy i odejścia klienta, zgodnie z prawami i obowiązkami wprowadzonymi aktem w sprawie danych.

Niniejsze standardowe postanowienia umowne łączą postanowienia dotyczące szczególnych kwestii bezpieczeństwa i ciągłości działania w całym procesie zmiany dostawcy, ze względu na zbliżony kontekst i cel obu tych obszarów. Chociaż w umowie o świadczenie usług zawarto postanowienia dotyczące bezpieczeństwa i ciągłości działania, istnieją pewne specyficzne aspekty związane z procesem zmiany dostawcy, które należy odzwierciedlić.

Proces zmiany dostawcy może powodować szczególne ryzyko dla bezpieczeństwa, które może wystąpić na różnych etapach procesu zmiany dostawcy w odniesieniu do jego poszczególnych aspektów, którym należy poświęcić szczególną uwagę, takich jak:

i. przetwarzanie danych,
ii. zarządzanie tożsamością i kontrola dostępu,
iii. przekazywanie danych,
iv. pobieranie danych,
v. bieżące zapewnienie poufności, integralności i dostępności danych oraz
vi. inne rodzaje ryzyka związane z przygotowaniem i realizacją skutecznego procesu zmiany dostawcy.

Podobnie szczególnej uwagi i rozważenia wymagają określone rodzaje ryzyka związane z ciągłością działania w odniesieniu do procesu zmiany dostawcy. Mogą one dotyczyć:

i. utrzymania ciągłości działania w celu zapewnienia wysokiego poziomu bezpieczeństwa usług,
ii. dalszego świadczenia usług na podstawie umowy,
iii. przedstawiania jasnych informacji o znanych zagrożeniach dla ciągłości świadczenia usług.

W tym względzie art. 25 ust. 2 lit. a) pkt (ii) aktu w sprawie danych nakłada na dostawcę obowiązek postępowania z należytą starannością w celu utrzymania ciągłości działalności oraz zapewnienia świadczenia funkcji lub usług przewidzianych w umowie. Dostawca jest również zobowiązany do przedstawienia jasnych informacji dotyczących znanych zagrożeń dla ciągłości świadczenia funkcji lub usług po stronie wyjściowego dostawcy usług przetwarzania danych (art. 25 ust. 2 lit. a) pkt (iii) aktu w sprawie danych).

Podejście do bezpieczeństwa i ciągłości działania oparte na analizie ryzyka: w zakresie, w jakim niniejsze standardowe postanowienia umowne przewidują ustalenia umowne, podejście do bezpieczeństwa oparte na analizie ryzyka i uwzględniające wszystkie rodzaje ryzyka oznacza dynamiczne i kontekstowe podejście do mających zastosowanie usług i modeli wdrażania oraz związanych z nimi sposobów wykorzystania, potrzeb i rodzajów ryzyka. Do klienta i dostawcy należy wspólne określenie, uzgodnienie, wdrożenie i monitorowanie powiązanych środków i kontroli w celu zapewnienia poprawy ogólnej odporności i integralności usług.

Na przykład należy zwrócić szczególną uwagę na ciągłe, odpowiednie i rozliczalne poziomy:

i. integralności danych,
ii. odporności na wszystkie znane podatności przy udostępnianiu danych do pobierania,
iii. podpisów szyfrujących,
iv. szczególnych mechanizmów kontroli dostępu z wykorzystaniem uwierzytelniania wieloskładnikowego,
v. weryfikacji tożsamości, w tym autoryzacji,

vi. bezpieczeństwa stron internetowych, portali, platform oraz powiązanych interfejsów programowania aplikacji (API),
vii. bezpieczeństwa po stronie dostawcy,
viii. zapewnienia i weryfikacji bezpieczeństwa po stronie klienta, w tym odpowiednich docelowych dostawców,
ix. działalności sieciowej,
x. ochrony przed atakami typu *brute force* przy rejestracji,
xi. bezpieczeństwa warstwy transportowej (TLS) oraz innych środków bezpieczeństwa danych w tranzycie,
xii. ochrony przed rozproszonym atakiem typu „odmowa usługi" (DDoS) oraz
xiii. solidnych polityk i praktyk kasowania danych.

Dostawca powinien być w stanie wykazać, z korzyścią dla klienta, że środki techniczne, operacyjne i organizacyjne w zakresie bezpieczeństwa oraz ochrony danych są zapewniane w sposób ciągły i odpowiedni.

Koncepcja ta jest podobna do struktury i podejścia określonych odpowiednio w (i) art. 25 RODO i art. 32 RODO [rozporządzenie (UE) 2016/679]; (ii) dyrektywie NIS 2 [EUR-Lex], (iii) programie certyfikacji cyberbezpieczeństwa na podstawie aktu o cyberbezpieczeństwie (UE) 2019/881.

Przykłady elementów, które dostawca powinien być w stanie wykazać, obejmują w szczególności:
i. wewnętrzne środki bezpieczeństwa, monitorowanie zapewnienia bezpieczeństwa oraz polityki dotyczące obsługi naruszeń bezpieczeństwa lub innych incydentów,
ii. zgodność z określonymi otwartymi, niezastrzeżonymi standardami powszechnie stosowanymi w danym sektorze,
iii. certyfikację lub inne formy zapewnienia zgodności albo spełnianie wymogów zgodności z właściwymi przepisami prawa krajowego lub z odpowiednimi europejskimi programami certyfikacji cyberbezpieczeństwa opracowanymi na podstawie rozporządzenia (UE) 2019/881 (akt o cyberbezpieczeństwie) lub
iv. regulacyjne standardy techniczne, o ile i w zakresie, w jakim mają one zastosowanie w danych sektorach.

Przepisy oparte na analizie ryzyka: w przypadku wielu dostawców działających w UE, a także niektórych klientów, zastosowanie mogą mieć pewne przepisy oparte na analizie ryzyka. Co do zasady prowadzi to do zwiększenia poziomu obowiązków i odpowiedzialności w zakresie bezpieczeństwa, a naruszenia i inne incydenty skutkują poważniejszymi konsekwencjami prawnymi, związanymi z reputacją i innymi kwestiami. W związku z tym zdecydowanie zaleca się uwzględnienie tych przepisów opartych na analizie ryzyka przed zawarciem umowy o świadczenie usług i podczas jej wykonywania.

Niektóre przykłady przepisów opartych na analizie ryzyka, które mogą mieć zastosowanie: dyrektywa NIS 2 (NIS 2), dyrektywa w sprawie odporności podmiotów krytycznych (CER), akt w sprawie operacyjnej odporności cyfrowej (DORA), akt dotyczący cyberodporności (CRA), akt o cyberbezpieczeństwie i ogólne rozporządzenie o ochronie danych (RODO), a także ewentualne przepisy prawa krajowego.

W niniejszych standardowych postanowieniach umownych używa się terminu „incydent" zarówno w odniesieniu do bezpieczeństwa, jak i ciągłości działania (*zob. sekcja „Definicje"*).

Klauzula 1.4 obejmuje na przykład również zgłoszenia na podstawie art. 33 RODO i art. 23 dyrektywy NIS 2.

Do niniejszego dokumentu dołączone są także inne standardowe postanowienia umowne zalecane przez Komisję, obejmujące szczególne zagadnienia inne niż bezpieczeństwo i ciągłość działania. Zachęca się strony do rozważenia stosowania również tych pozostałych klauzul, ponieważ zostały opracowane tak, aby były spójne i wzajemnie się uzupełniały.

1. **Bezpieczeństwo i ciągłość działania**

1.1. **Kwestie ogólne**

1.1.1. Dostawca zobowiązuje się stosować najbardziej odpowiednie środki techniczne i organizacyjne, aby zagwarantować, że poziom bezpieczeństwa i odporności jest proporcjonalny do ryzyka stwarzanego przez usługi oraz ich zamierzone i dające się racjonalnie przewidzieć wykorzystanie w kontekście procesu zmiany dostawcy.

1.1.2. Ponadto dostawca zobowiązuje się zapobiegać zakłóceniom świadczenia usług oraz utrzymywać ciągłość usług podczas procesu zmiany dostawcy. Obejmuje to posiadanie i utrzymywanie odpowiedniego zarządzania ciągłością działania, które obejmuje planowanie awaryjne i środki przywracania sprawności po wystąpieniu sytuacji nadzwyczajnej w oparciu o utrwalone najlepsze praktyki i standardy rynkowe. Środki te muszą być aktualizowane oraz okresowo poddawane przeglądowi i testowane przez dostawcę.

1.2. **Bezpieczeństwo**

1.2.1. Zgodnie z klauzulą 1.1.1 dostawca jest zobowiązany wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia utrzymania wysokiego poziomu bezpieczeństwa podczas procesu zmiany dostawcy. Dotyczy to w szczególności bezpieczeństwa danych podczas ich przekazywania i dalszego bezpieczeństwa danych podczas okresu zatrzymywania.

1.2.2. Dostawca jest zobowiązany wdrożyć odpowiednie środki techniczne i organizacyjne w celu utrzymania podczas procesu zmiany dostawcy poziomu bezpieczeństwa proporcjonalnego do poziomu ryzyka. Obejmuje to: istotne ryzyko związane z bezpieczeństwem przetwarzania danych, zarządzaniem tożsamością i kontrolą dostępu, możliwością przenoszenia danych, pobieraniem danych, bieżącą poufnością, integralnością i dostępnością danych, a także wszelkie inne ryzyko związane ze skuteczną zmianą dostawcy.

1.2.3. Środki objęte klauzulami 1.1.1 oraz 1.2.1 muszą zapewniać co najmniej, bez ograniczeń:

a) ciągłą poufność, integralność i dostępność danych oraz odporność usług, danych eksportowalnych i aktywów cyfrowych,

b) przywrócenie dostępności i integralności danych oraz dostępu do nich w rozsądnym terminie w przypadku incydentu oraz

c) ciągłe monitorowanie oraz regularne testowanie, ocenę i ewaluację skuteczności środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa usług, danych eksportowalnych i aktywów cyfrowych.

1.3. **Ciągłość działania**

1.3.1. Zgodnie z klauzulą 1.1.2 dostawca jest zobowiązany w szczególności:

a) postępować z należytą starannością w celu utrzymania ciągłości działalności i kontynuować świadczenie usług przewidzianych w umowie oraz

b) przekazywać jasne informacje o znanych zagrożeniach dla ciągłości świadczenia usług.

1.4. **Zawiadomienia**

1.4.1. Strony uzgadniają, że wszelkie zawiadomienia między nimi w odniesieniu do tych klauzul dotyczących bezpieczeństwa i ciągłości działania będą dokonywane [*strony wskazują wybrane środki komunikacji, z uwzględnieniem odpowiednich środków elektronicznych*].

1.4.2. Dostawca jest zobowiązany zawiadamiać klienta o wszelkich incydentach. Dostawca jest zobowiązany zawiadomić o incydencie bez zbędnej zwłoki, a w każdym razie w ciągu 72 (siedemdziesięciu dwóch) godzin od powzięcia wiadomości o incydencie, chyba że obowiązki regulacyjne wymagają ostrzeżenia lub podobnego zawiadomienia w krótszym terminie.

1.4.3. Zawiadomienie dostawcy musi zawierać informacje niezbędne klientowi do oceny skutków incydentu. Dostawca jest zobowiązany niezwłocznie, skutecznie, w uzasadnionym zakresie i bez dodatkowych kosztów udzielać pomocy klientowi i współpracować z nim (w tym z osobami trzecimi upoważnionymi przez klienta) w związku z wszelkimi czynnościami dochodzeniowymi, do których podjęcia klient jest uprawniony zgodnie z mającym zastosowanie prawem unijnym i krajowym.

1.4.4. W przypadku gdy incydent ma lub może mieć wpływ na dostawcę, dostawca jest zobowiązany podjąć najbardziej odpowiednie działania niezbędne do zminimalizowania skutków incydentu i zapobieżenia jego ponownemu wystąpieniu. Nie ma to wpływu na inne prawa, które mogą przysługiwać klientowi na mocy umowy lub na mocy mającego zastosowanie prawa unijnego lub krajowego.

1.5. **Pozostałe postanowienia**

1.5.1. Na wniosek klienta dostawca jest zobowiązany bez zbędnej zwłoki przekazać klientowi podsumowanie kluczowych elementów środków bezpieczeństwa stosowanych przez dostawcę i związanego z nimi zarządzania bezpieczeństwem, a także ciągłości działania dostawcy i związanego z nią zarządzania w sytuacjach awaryjnych oraz wszelkich istotnych zmian w odniesieniu do któregokolwiek z powyższych.

1.5.2. Na wniosek klienta dostawca jest zobowiązany bez zbędnej zwłoki przekazać klientowi dodatkowe informacje uzupełniające wspomniane powyżej podsumowanie, takie jak wyniki testów i dowody wiarygodności. W takim przypadku dostawca może zażądać od klienta podpisania umowy o zachowanie poufności przed udostępnieniem takich szczegółowych informacji. Umowa o zachowanie poufności musi jednak zawierać zwyczajowe wyjątki i pozostawać bez wpływu na pozostałe postanowienia niniejszego akapitu, umowę oraz mające zastosowanie prawo unijne lub krajowe. Dostawca ma prawo żądać, aby szczegółowe informacje były udostępniane wyłącznie na zasadzie ograniczonego dostępu, w tym wyznaczonym dostawcom lub innym odpowiednim dostawcom klienta będącym osobami trzecimi.

Do takich zwyczajowych wyjątków należą wszelkie (odpowiednie części) informacji, które: (i) są już publicznie dostępne, (ii) klient jest zobowiązany ujawnić, jeżeli jest to obowiązkowe a) na mocy prawa właściwego lub b) na żądanie organu rządowego lub innego organu regulacyjnego (w tym w szczególności, bez ograniczeń, na podstawie orzeczenia sądu, RODO lub dyrektywy NIS 2).

1.6. **Pierwszeństwo**

Bez uszczerbku dla standardowych klauzul umownych na mocy RODO, w przypadku jakiejkolwiek sprzeczności lub niespójności między niniejszymi klauzulami dotyczącymi bezpieczeństwa i ciągłości działania a innymi mającymi zastosowanie ustaleniami umownymi, postanowieniami, warunkami lub innymi umowami odnoszącymi się do bezpieczeństwa i ciągłości działania pierwszeństwo mają niniejsze klauzule.

ZAŁĄCZNIK IX

STANDARDOWE POSTANOWIENIA UMOWNE

dotyczące unikania rozproszenia

Umowy o przetwarzanie danych często obejmują różne dokumenty pomocnicze odsyłające do dodatkowych materiałów i informacji, które mogą być rozproszone w różnych repozytoriach. Utrudnia to potencjalnym klientom znalezienie wszystkich informacji, których potrzebują do oceny zobowiązań umownych i obowiązków prawnych stron oraz ich skutków.

W kontekście procesu zmiany dostawcy bardzo ważna jest przejrzystość. Przyszły klient potrzebuje łatwego dostępu do istotnych aktualnych informacji, dokumentów, materiałów i danych kontaktowych, nawet przed zawarciem umowy z dostawcą. Standardowe postanowienia umowne dotyczące unikania rozproszenia zapewniają symetrię informacyjną i komunikacyjną.

Ułatwiają zarówno klientowi, jak i dostawcy łatwy i praktyczny dostęp do odpowiednich, aktualnych informacji, dokumentów, materiałów i danych kontaktowych. Mają one na celu stworzenie środowiska sprzyjającego przejrzystości między stronami oraz zapewnienie, aby nie istniały żadne przeszkody umowne utrudniające zmianę dostawcy, przez umożliwienie klientowi znalezienia w umowie wszystkich istotnych i aktualnych informacji na temat jego praw i obowiązków. Przyczyni się to do powstania sprawiedliwego i zrównoważonego stosunku prawnego między klientem a dostawcą oraz szerzej – do sprawiedliwości umownej, zgodnie z założeniami rozporządzenia (UE) 2023/285 (zwanego dalej „aktem w sprawie danych").

Do niniejszego dokumentu dołączone są także inne standardowe postanowienia umowne zalecane przez Komisję, obejmujące szczególne zagadnienia inne niż unikanie rozproszenia. Zachęca się strony do rozważenia stosowania również tych pozostałych klauzul, ponieważ zostały opracowane tak, aby były spójne i wzajemnie się uzupełniały.

1. **Unikanie rozproszenia**

1.1. **Warunki i ustalenia wstępne**

1.1.1. Dostawca zapewnia, aby wszystkie ustalenia umowne były łatwo, szybko i stale dostępne dla klienta a) w jednej specjalnej bezpiecznej lokalizacji online oraz b) w zrozumiałym formacie, nadającym się do odczytu przez człowieka i odczytu maszynowego. Ponadto dostawca zapewnia, aby ustalenia umowne mogły być pobrane lub w inny sposób wyeksportowane przez klienta w kompletnej i uporządkowanej formie.

1.1.2. Ustalenia umowne muszą obejmować co najmniej:

a) **nazwę i adres:** pełną oficjalną nazwę przedsiębiorstwa dostawcy jako osoby prawnej, w tym m.in. jego oficjalną formę prawną, krajowy numer rejestracyjny, pełny adres siedziby oraz numer identyfikacyjny VAT;

b) **aktualną umowę:** aktualną, opatrzoną znacznikiem czasu umowę (oraz, w miarę dostępności, odpisy umowy), w tym wszystkie postanowienia, przyjęte oferty, warunki, polityki, informacje, dokumentację, harmonogramy, wykazy i załączniki, które mają zastosowanie między dostawcą a klientem;

c) **zapis historyczny:** historyczny zapis umów opatrzonych znacznikiem czasu, w miarę możliwości w połączeniu z wszelkimi dodatkowymi postanowieniami, warunkami, w tym wszelkimi politykami, informacjami, wszelką dokumentacją, wszelkimi harmonogramami, wykazami, załącznikami lub innymi dokumentami, które miały zastosowanie między dostawcą a klientem, w tym:

(i) dowody dozwolonych jednostronnych zmian i odpowiednie daty ich wejścia w życie określone w standardowych postanowieniach umownych dotyczących niewprowadzania zmian;

W odniesieniu do dozwolonych jednostronnych zmian oraz odpowiednich dat ich wejścia w życie zob. standardowe postanowienia umowne dotyczące niewprowadzania zmian.

d) **ekosystem przetwarzania i dostarczania danych:** aktualny zapis historyczny oraz szczegółowy wykaz podwykonawców, podmiotów przetwarzających dane lub innych odpowiednich zainteresowanych stron z ekosystemu łańcucha dostaw dostawcy, w tym nazwy oraz adresy, jak w klauzuli 1.1.2 lit. a) powyżej;

e) **dane kontaktowe:** aktualne dane kontaktowe dostawcy, w tym szczegółowe informacje na temat funkcji głównej osoby kontaktowej, głównej osoby kontaktowej ds. technicznych oraz głównej osoby kontaktowej ds. umownych i administracyjnych, obejmujące odpowiednie nazwy stanowisk, numery telefonów oraz adresy e-mail uzgodnione przez strony;

f) **sprawozdawczość w zakresie wyników operacyjnych:** jeżeli jest to technicznie wykonalne – aktualny, a także historyczny przegląd sprawozdawczości w zakresie wyników operacyjnych sporządzanej przez dostawcę w odniesieniu do świadczonej usługi oraz innych obowiązków wynikających z umowy oraz

g) **zawiadomienia:** wszelkie zawiadomienia prawne i inne istotne zawiadomienia opatrzone znacznikiem czasu przekazywane między stronami lub stronie, związane z ustaleniami umownymi, o których mowa w klauzuli 1.1.2 lit. a) i b).

W kilku sytuacjach akt w sprawie danych zobowiązuje dostawcę do przekazywania wymaganych informacji klientowi. Obowiązki te znajdują odzwierciedlenie w odpowiednich standardowych postanowieniach umownych. Na przykład informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych (art. 26 aktu w sprawie danych) są zawarte w standardowych postanowieniach umownych dotyczących zmiany dostawcy i odejścia klienta; obowiązek przedstawiania jasnych informacji o znanych zagrożeniach dla ciągłości świadczenia funkcji/usług znajduje odzwierciedlenie w standardowych postanowieniach umownych dotyczących bezpieczeństwa i ciągłości działania oraz w standardowych postanowieniach umownych dotyczących zmiany dostawcy i odejścia klienta.

1.2. **Pierwszeństwo**

W przypadku jakiejkolwiek sprzeczności lub niespójności między niniejszymi klauzulami dotyczącymi unikania rozproszenia mającej zastosowanie dokumentacji umownej a innymi mającymi zastosowanie ustaleniami umownymi, postanowieniami, warunkami lub innymi umowami odnoszącymi się do przedmiotu niniejszych klauzul pierwszeństwo mają niniejsze klauzule.

ZAŁĄCZNIK X

STANDARDOWE POSTANOWIENIA UMOWNE

dotyczące odpowiedzialności

Chociaż klauzula dotycząca odpowiedzialności jest zazwyczaj zawarta w ogólnej umowie między klientem a dostawcą, postanowienia niniejszych standardowych postanowień umownych dotyczących odpowiedzialności odzwierciedlają ducha rozporządzenia (UE) 2023/2854 (zwanego dalej aktem w sprawie danych) w odniesieniu do znaczenia sprawiedliwych, zasadnych i niedyskryminujących praw i obowiązków i jako takie mogą być użytecznym uzupełnieniem standardowych postanowień umowy dotyczących odpowiedzialności.

W związku z tym zaleca się włączenie takiej klauzuli, ponieważ ma ona zasadnicze znaczenie dla równowagi stosunków umownych między stronami i stanowi zachętę do przestrzegania praw i obowiązków uzgodnionych przez strony. W szczególności małe i średnie przedsiębiorstwa oraz inne organizacje mogą uznać te standardowe postanowienia umowne za pomocne przy uzgadnianiu postanowień dotyczących odpowiedzialności w swoich umowach. Klient i dostawca mogą swobodnie uzgodnić w umowie dodatkowe prawa i obowiązki. Zastosowanie tej klauzuli nie zwalnia stron z obowiązku zapewnienia zgodności z wszelkimi mającymi zastosowanie bezwzględnie obowiązującymi przepisami prawa UE lub prawa krajowego oraz odpowiedniego dostosowania umowy.

Przed zawarciem umowy klient może sprawdzić rynek ubezpieczeń, tak aby wybrać najodpowiedniejszy dla siebie produkt ubezpieczeniowy. Zaleca się zasięgnięcie porady eksperta specjalizującego się w ubezpieczeniach.

Do niniejszego dokumentu dołączone są także inne standardowe postanowienia umowne zalecane przez Komisję, obejmujące szczególne zagadnienia inne niż odpowiedzialność. Zachęca się strony do rozważenia stosowania również tych pozostałych klauzul, ponieważ zostały opracowane tak, aby były spójne i wzajemnie się uzupełniały.

Nieograniczona odpowiedzialność

Co do zasady każda strona umowy powinna ponosić nieograniczoną odpowiedzialność w przypadkach umyślnego działania, umyślnego naruszenia przepisów lub rażącego niedbalstwa, w tym naruszenia przez stronę obowiązku zachowania poufności danych drugiej strony lub obowiązku niewykorzystywania danych do celów innych niż cele wyraźnie uzgodnione przez strony.

W standardowych postanowieniach umownych zaleca się oddzielenie przypadków umyślnego działania od przypadków umyślnego naruszenia przepisów oraz jednoznaczne wskazanie, że wszelkie działania umyślne są objęte zakresem tej odpowiedzialności, niezależnie od prawa właściwego dla umowy. W niektórych jurysdykcjach umyślne naruszenie przepisów może być tożsame z umyślnym działaniem. W takich przypadkach strony mogą podjąć decyzję o niewprowadzaniu rozróżnienia między umyślnym naruszeniem przepisów a umyślnym działaniem.

Zwolnienia z nieograniczonej odpowiedzialności

Usługi przetwarzania danych świadczone przez ograniczony okres jako nieprzeznaczona do produkcji wersja do celów testowania i oceny (art. 31 ust. 2 aktu w sprawie danych) zazwyczaj nie są przeznaczone do przetwarzania danych wrażliwych (np. tajemnic przedsiębiorstwa, danych osobowych lub rzeczywistych danych dotyczących produkcji). Takie wersje nieprzeznaczone do produkcji zasadniczo nie są również wystarczająco rozwinięte do takiego przetwarzania i nie mają zdolności, mechanizmów kontroli ani konfiguracji, których można by zasadnie oczekiwać w wersji przeznaczonej do produkcji. Zdecydowanie odradza się klientowi przetwarzanie rzeczywistych danych dotyczących produkcji w takich wersjach nieprzeznaczonych do produkcji. W tych standardowych postanowieniach umownych proponuje się, aby klient – jeżeli mimo to zdecyduje się na takie przetwarzanie – czynił to na własne ryzyko, a dostawca nie ponosił odpowiedzialności w przypadku naruszenia poufności danych w takich sytuacjach. W takiej sytuacji zastosowanie mogą mieć szczególne ustalenia dotyczące odpowiedzialności uzgodnione przez strony.

Podobnie w akcie w sprawie danych przewidziano sytuacje, w których niektóre obowiązki nie mają zastosowania do usług, w przypadku których większość głównych cech została opracowana na zamówienie, gdy wszystkie komponenty zostały opracowane na potrzeby indywidualnego klienta, lub usług świadczonych w środowisku nieprodukcyjnym. W związku z tym odpowiedzialność w takich przypadkach również musiałaby zostać wyraźnie uzgodniona.

Ograniczona odpowiedzialność

Zgodnie z obecną praktyką biznesową strony zgadzają się ograniczyć swoją odpowiedzialność (w szczególności odpowiedzialność dostawcy) w niektórych przypadkach. W poniższych standardowych postanowieniach umownych zaproponowano trzy główne warianty ograniczenia odpowiedzialności:

— **Wariant A:** odpowiedzialność jest ograniczona do kwoty określonej przez strony na podstawie oceny ryzyka. W ramach tego wariantu obie strony przeprowadzają ocenę ryzyka i przekazują swoje ustalenia drugiej stronie na etapie poprzedzającym zawarcie umowy. Druga strona może odrzucić otrzymaną ocenę ryzyka. W przypadku odrzucenia oceny ryzyka strony mogą zastosować jeden z pozostałych wariantów ograniczenia odpowiedzialności.

Mogą wystąpić zmiany w wolumenie usług świadczonych przez dostawcę, a także zmiana zakresu (dodanie nowych usług lub usunięcie niektórych usług). Może to wymagać zmian w ocenie ryzyka, a strony powinny dostosować limit odpowiedzialności, tak aby odzwierciedlał rzeczywistą sytuację w zakresie ryzyka. Zachęca się strony do sprawdzenia przykładowego wzoru oceny ryzyka w wariancie A, tak aby były świadome ryzyka związanego z usługami przetwarzania danych w odniesieniu do ich konkretnej działalności;

— **wariant B**: odpowiedzialność jest ograniczona do szkód bezpośrednich. Szkody pośrednie, takie jak utracone korzyści lub utrata potencjalnych oszczędności, są wyłączone. Wariant ten można również połączyć z wariantami A i C (tj. odpowiedzialność ograniczona do szkód bezpośrednich, ale nie wyższa niż kwota ustalona przez strony określona w wyniku oceny ryzyka albo ustalona na innej podstawie);

— **wariant C**: odpowiedzialność stron jest ograniczona do wcześniej uzgodnionej maksymalnej kwoty, którą można obliczyć na przykład na podstawie (i) równowartości jednej lub kilku rocznych opłat (uiszczonych i należnych) od klienta na rzecz dostawcy; (ii) zakresu ochrony ubezpieczeniowej wykupionej przez dostawcę w odniesieniu do usług; (iii) maksymalnej kwoty objętej ogólnym ubezpieczeniem odpowiedzialności zawodowej dostawcy lub (iv) połączenia różnych wzorów, np. wzoru powiązanego z wartością pieniężną usług pomnożoną przez kwotę równą łącznym rocznym opłatom (uiszczonym albo jeszcze należnym na podstawie umowy) za te usługi.

Zabezpieczenie przed roszczeniami: te standardowe postanowienia umowne nie zawierają postanowień dotyczących zabezpieczenia przed roszczeniami. Zachęca się strony do rozważenia, czy – a jeżeli tak, to w jakim zakresie – jedna strona powinna zobowiązać się do zabezpieczenia drugiej strony przed roszczeniami osób trzecich oraz zwolnienia jej z odpowiedzialności z tytułu takich roszczeń, wynikających z istotnego naruszenia zobowiązań na podstawie umowy przez działania lub zaniechania strony odpowiedzialnej, jej pracowników, przedstawicieli lub podwykonawców. W przypadku klientów zabezpieczenie roszczeń może dotyczyć na przykład naruszenia przez dostawcę obowiązków zachowania poufności, niewykorzystywania danych lub naruszenia praw własności intelektualnej osób trzecich. W przypadku dostawców zabezpieczenie roszczeń może obejmować naruszenie przez klienta praw własności intelektualnej osób trzecich lub roszczenia osób trzecich wobec dostawcy związane z hostowaniem przez klienta nielegalnych treści.

1. Odpowiedzialność

1.1. Nieograniczona odpowiedzialność

1.1.1. W przypadkach naruszenia zobowiązań wynikających z niniejszej umowy w drodze umyślnego działania, umyślnego naruszenia przepisów lub rażącego niedbalstwa strona, która dopuściła się naruszenia, ponosi odpowiedzialność za wszelkie szkody, z zastrzeżeniem klauzuli 1.2 poniżej. [WARIANT] [Z wyjątkiem przypadków określonych w klauzuli 1.2 dostawca ponosi nieograniczoną odpowiedzialność za wszelkie szkody wyrządzone klientowi w wyniku naruszenia poufności danych klienta przetwarzanych na podstawie niniejszej umowy.]

1.1.2. W przypadku naruszenia obowiązku niewykorzystywania danych strony do celów innych niż cele wyraźnie uzgodnione przez strony strona, która dopuściła się naruszenia, ponosi nieograniczoną odpowiedzialność za wszelkie szkody.

Celem wariantu przewidzianego w klauzuli 1.1.1 jest zagwarantowanie poufności wszystkich danych klienta zgodnie z prawami i obowiązkami dotyczącymi poufności oraz w zakresie uzgodnionym w umowie. Zgodnie z mającym zastosowanie prawem (np. RODO, NIS 2 itp.) odbiorca informacji poufnych może być zobowiązany do ujawnienia pewnych informacji określonym osobom lub organizacjom do celów uzgodnionych i wyraźnie opisanych w umowie.

1.2. Zwolnienia z nieograniczonej odpowiedzialności

1.2.1. Jeżeli strony uzgodnią nieograniczoną odpowiedzialność zgodnie z klauzulą 1.1.1, nieograniczona odpowiedzialność dostawcy nie ma zastosowania do danych klienta w ramach usług przetwarzania danych dostawcy świadczonych jako wersja nieprzeznaczona do produkcji.

Zob. art. 31 ust. 2 aktu w sprawie danych oraz nota wyjaśniająca „Zwolnienia z nieograniczonej odpowiedzialności” zawarta w niniejszych standardowych postanowieniach umownych.

1.2.2. Dostawca nie ponosi odpowiedzialności za:

a) obowiązki niemające zastosowania do usług przetwarzania danych na podstawie (i) art. 23 lit. d) aktu w sprawie danych (uzyskanie równoważności funkcjonalnej), (ii) art. 29 (stopniowe wycofywanie opłat z tytułu zmiany dostawcy) lub (iii) art. 30 ust. 1 i 3 aktu w sprawie danych (techniczne aspekty zmiany dostawcy), w przypadku których większość głównych cech została opracowana na zamówienie, tak aby dostosować je do konkretnych potrzeb klienta lub w przypadku których wszystkie komponenty zostały opracowane na potrzeby klienta oraz jeżeli te usługi przetwarzania danych nie są oferowane komercyjnie na szeroką skalę przez katalog usług przetwarzania danych. Zwolnienie ma zastosowanie, jeżeli dostawca poinformował klienta przed zawarciem umowy o świadczenie usług przetwarzania danych, że wskazane powyżej przepisy aktu w sprawie danych nie mają zastosowania do danych usług;

b) naruszenie obowiązków związanych ze zmianą dostawcy usług przetwarzania danych w przypadku usług przetwarzania danych świadczonych przez ograniczony okres jako nieprzeznaczona do produkcji wersja do celów testowania i oceny.

1.3. **Ograniczona odpowiedzialność**

Wariant A: Kwota określona na podstawie oceny ryzyka

1.3.1. Strony postanawiają ograniczyć swoją odpowiedzialność za nieumyślne naruszenie zobowiązań na podstawie niniejszej umowy do kwoty […] za zdarzenie, przy czym szereg zdarzeń powiązanych traktuje się jako jedno zdarzenie. Kwotę określa w dobrej wierze strona poszkodowana, na podstawie oceny ryzyka lub innych szacunków uzgodnionych przez strony w załączniku 1 (wzór oceny ryzyka). Ocenę ryzyka przeprowadza się i przekazuje drugiej stronie [.... dni] przed zawarciem umowy. Jeżeli druga strona nie odrzuci oceny ryzyka, umowa zostaje zawarta w oparciu o tę ocenę.

Strony mogą w dowolnym momencie uzgodnić przeprowadzenie ponownej oceny ryzyka w celu odzwierciedlenia zmian sytuacji w zakresie ryzyka w odniesieniu do usług. W tym celu mogą skorzystać ze wzoru przedstawionego w przykładzie [wzór oceny ryzyka]. Jeżeli ponowna ocena skutkuje zwiększeniem lub zmniejszeniem ryzyka dla strony, strona ta może zwrócić się z wnioskiem o renegocjację limitu odpowiedzialności za usługi w celu odzwierciedlenia zmiany związanego z nimi ryzyka lub dodatkowych warunków, które powinny zostać spełnione, w tym warunków cenowych lub zmian umowy o gwarantowanym poziomie usług. Strony mogą uzgodnić, że jeżeli porozumienia nie uda się osiągnąć w terminie [trzech miesięcy od dnia złożenia wniosku przez stronę], pierwotnie uzgodniony limit odpowiedzialności pozostaje bez zmian.

Wariant B: Szkody bezpośrednie

1.3.2. Strony postanawiają ograniczyć swoją odpowiedzialność za nieumyślne naruszenie zobowiązań na podstawie niniejszej umowy wyłącznie do szkód bezpośrednich.

1.3.3. Szkody bezpośrednie obejmują również: (i) koszty poniesione w celu ustalenia przyczyny i zakresu szkody, (ii) koszty poniesione przez stronę poszkodowaną w celu zapobieżenia szkodom bezpośrednim lub ich ograniczenia, pod warunkiem że koszty te rzeczywiście doprowadziły do zapobieżenia tym szkodom lub ich ograniczenia, (iii) szkodę wynikającą z uszkodzenia, niedostępności lub utraty danych oraz (iv) koszty poniesione przez jedną ze stron w celu zapewnienia zgodności usług z poziomami wykorzystania uzgodnionymi w umowie, jeżeli druga strona nie usunęła takiego naruszenia w uzgodnionym terminie.

1.3.4. W przypadku gdy szereg zdarzeń powiązanych traktuje się jako jedno zdarzenie, łączna odpowiedzialność jednej strony wobec drugiej strony z tytułu takich szkód bezpośrednich, o których mowa w poprzednim zdaniu, jest ograniczona do kwoty […].

Wariant C: Kwota maksymalna

1.3.5. Strony postanawiają ograniczyć swoją odpowiedzialność za nieumyślne naruszenie zobowiązań na podstawie niniejszej umowy – w tym w sytuacji, gdy szereg zdarzeń powiązanych traktuje się jako jedno zdarzenie – do maksymalnej kwoty […].

1.4. **Zawiadomienia**

Strony uzgadniają, że wszelkie zawiadomienia między nimi w odniesieniu do klauzul dotyczących odpowiedzialności będą dokonywane (*strony wskazują wybrane środki komunikacji, z uwzględnieniem odpowiednich środków elektronicznych*).

1.5. **Pierwszeństwo**

W przypadku jakiejkolwiek sprzeczności lub niespójności między niniejszymi klauzulami dotyczącymi odpowiedzialności a innymi mającymi zastosowanie ustaleniami umownymi, postanowieniami, warunkami lub innymi umowami odnoszącymi się do odpowiedzialności w zakresie objętym niniejszymi klauzulami pierwszeństwo mają niniejsze klauzule.

Dodatek 1

Wzór oceny ryzyka

W celu określenia ryzyka związanego z usługą strona przeprowadza ocenę, uwzględniając szczególne ryzyko nieumyślnego niewykonania zobowiązania umownego przez drugą stronę.

Ocenę ryzyka należy przeprowadzić w dobrej wierze. Powinna ona realistycznie odzwierciedlać potencjalne szkody. Jeżeli oszacowane kwoty są zbyt niskie, odpowiedzialność za szkody przekraczające te kwoty zostaje wyłączona. Jeżeli oszacowane kwoty są zbyt wysokie, druga strona może odmówić przyjęcia odpowiedzialności lub zażądać wyższych kosztów.

W razie potrzeby można uwzględnić dodatkowe ryzyka.

Opis ryzyka		Oszacowanie szkody
Zakłócenie działalności gospodarczej Utrata obrotów spowodowana naruszeniem umowy. Można rozważyć potencjalną przerwę w świadczeniu usług oraz jej skutki dla działalności lub operacji strony.	EUR	
Odzyskiwanie danych Zakładane koszty odzyskiwania utraconych, niedostępnych lub uszkodzonych danych. Strony mogą być zobowiązane do wdrożenia środków ograniczających ryzyko, np. przez posiadanie kopii zapasowych danych u innego dostawcy lub w lokalnej infrastrukturze.	EUR	
Kary administracyjne Kary pieniężne nakładane przez organy publiczne na przedsiębiorstwa, na przykład grzywny za naruszenie przepisów o ochronie danych lub przepisów regulacyjnych, związane ze świadczeniem usługi przez dostawcę.	EUR	
Utrata tajemnic przedsiębiorstwa Ujawnienie tajemnic przedsiębiorstwa może prowadzić do utraty możliwości rynkowych. Za takie szkody można dochodzić odszkodowania na podstawie przepisów prawa.	EUR	
Naruszenie ochrony danych osobowych i działania naprawcze Naruszenie ochrony danych osobowych może prowadzić do powstania różnych rodzajów kosztów bezpośrednich, w tym kosztów obsługi prawnej, kosztów postępowań sądowych oraz kosztów działań naprawczych dotyczących danych mających na celu usunięcie problemów z jakością danych związanych z naruszeniem.	EUR	
Utrata reputacji Strony mogą rozważyć wpływ na reputację przedsiębiorstwa oraz środki, które będą konieczne (np. działania reklamowe lub kampanie informacyjne w celu zrekompensowania wpływu na reputację). Odzyskanie takich kosztów w pełnej wysokości w postępowaniu sądowym może być trudne.	EUR	
Odpowiedzialność wobec osób trzecich Odpowiedzialność wobec osób trzecich obejmuje potencjalną odpowiedzialność, na przykład wobec dostawców, klientów, podwykonawców i osób trzecich.	EUR	
Łączne ryzyko potencjalnych szkód (suma)	**EUR**	

Ponieważ usługi przetwarzania danych są świadczone w sposób skalowalny i elastyczny, zarówno korzystanie z usługi świadczonej przez dostawcę, jak i ryzyko odpowiedzialności mogą zmieniać się w trakcie obowiązywania umowy, często w zakresie określonym w umowach o gwarantowanym poziomie usług. Zaleca się, aby przy ocenie ryzyka w momencie zawierania umowy lub regularnie strony uwzględniały – oprócz potencjalnych maksymalnych teoretycznych szkód – zmieniający się charakter i wolumen usług. Pozwala to na ustalenie bardziej realistycznej wartości odpowiadającej średniemu lub oczekiwanemu poziomowi korzystania z usług. Strony powinny również dostosować ocenę do swoich procesów planowania wewnętrznego. Nie wszystkie wymienione kategorie ryzyka muszą w równym stopniu dotyczyć klienta i dostawcy, czy też określonej linii biznesowej klienta.

ZAŁĄCZNIK XI

STANDARDOWE POSTANOWIENIA UMOWNE

dotyczące niewprowadzania zmian

Ważne jest, aby strony mogły polegać na uzgodnionych umownie prawach i obowiązkach oraz aby te prawa i obowiązki nie były zmieniane jednostronnie, chyba że na jasno i wspólnie uzgodnionych warunkach. Jest to szczególnie ważne w przypadku małych i średnich przedsiębiorstw lub innych organizacji, które mogą nie dysponować wystarczającymi zasobami do oceny możliwego wpływu takich jednostronnych zmian na ich działalność i zadania. Standardowe postanowienia umowne dotyczące niewprowadzania zmian mają na celu zapewnienie stronom większej jasności i pewności przy uzgadnianiu postanowień odnoszących się do jednostronnych zmian. Te standardowe postanowienia umowne odnoszą się do odpowiednich scenariuszy i możliwych ustaleń umownych związanych z nimi. Ich celem jest zapewnienie, aby takie jednostronne zmiany nie były szkodliwe dla interesów żadnej ze stron.

Podejście do jednostronnych zmian

Co do zasady żadna ze stron nie może jednostronnie zmienić umowy (w tym standardowych postanowień umownych), a wszelkie zmiany wymagają wzajemnego uzgodnienia. Jedynie w ściśle określonych warunkach przewidzianych w niniejszych standardowych postanowieniach umownych dopuszcza się pewne jednostronne zmiany. Znajduje to odzwierciedlenie w klauzulach od 1.1.1 do 1.1.3 niniejszych standardowych postanowień umownych.

W tych standardowych postanowieniach umownych uznaje się, że w pewnych okolicznościach dostawca powinien mieć możliwość proponowania jednostronnych zmian świadczonych usług. Zmiany te określane są jako dozwolone jednostronne zmiany i zostały uregulowane w klauzulach od 1.1.3 do 1.1.6 niniejszych standardowych postanowień umownych. Dozwolone jednostronne zmiany można zaproponować tylko raz i muszą one spełniać następujące warunki:

1) poprawiają pozycję klienta w zakresie korzystania z usługi z perspektywy umownej, finansowej, organizacyjnej, operacyjnej, poziomu świadczenia usług, zgodności z prawem lub z innego istotnego punktu widzenia oraz
2) zostaną zakomunikowane klientowi nie później niż 30 dni kalendarzowych przed dniem, w którym taka dozwolona jednostronna zmiana miałaby stać się skuteczna wobec klienta.

Taki termin zawiadomienia umożliwi klientowi ocenę informacji, a także wykonalności i wpływu zmiany na klienta oraz zainteresowane strony, systemy i usługi klienta.

Do niniejszego dokumentu dołączone są także inne standardowe postanowienia umowne zalecane przez Komisję, obejmujące szczegółowe zagadnienia inne niż niewprowadzanie zmian. Zachęca się strony do rozważenia stosowania również tych pozostałych klauzul, ponieważ zostały opracowane tak, aby były spójne i wzajemnie się uzupełniały.

1. **Niewprowadzanie zmian**

1.1. **Zmiana**

1.1.1. Każda zmiana umowy („zmiana”) musi zostać dokonana na piśmie, w tym za pomocą odpowiednich środków elektronicznych, i wymaga uprzedniej wzajemnej zgody stron, w tym również wyrażonej za pomocą odpowiednich środków elektronicznych.

1.1.2. Niezależnie od klauzuli 1.1.1 dostawca jest uprawniony do zmiany umowy, jeżeli jest to wymagane do zapewnienia zgodności z mającym zastosowanie bezwzględnie obowiązującym prawem, które nie obowiązywało przed datą wejścia w życie umowy.

1.1.3. Z zastrzeżeniem klauzuli 1.1.2 dostawca jest uprawniony do zaproponowania jednostronnej zmiany usług jedynie pod warunkiem że:

a) taka zmiana jest korzystna dla klienta usług przetwarzania danych, ponieważ polega na przykład na istotnych aktualizacjach usprawniających usługę lub jest konieczna ze względów bezpieczeństwa, oraz

b) wszystkie warunki określone w klauzulach od 1.1.4 do 1.1.6 („dozwolona jednostronna zmiana”) zostały spełnione.

1.1.4. Dostawca nie może wykorzystać żadnej proponowanej jednostronnej zmiany na podstawie klauzuli 1.1.3 do bezpośredniego ani pośredniego wprowadzania lub egzekwowania zmian z mocą wsteczną, ani do zmiany postanowień umowy dotyczących w szczególności następujących kwestii:

a) wyboru prawa właściwego i sądu właściwego,

b) zmiany umowy lub procedury zmiany umowy,

c) okresu obowiązywania i rozwiązania umowy,

d) odpowiedzialności,

e) poufności,

f) metod korzystania z podwykonawstwa i metod zmiany podwykonawców,

g) praw dostępu i praw do informacji,

h) jakościowych celów w zakresie poziomu świadczenia usług,

Zmiany dotyczące już uzgodnionych ilościowych i jakościowych celów w zakresie skuteczności wykonania usług w ramach uzgodnionych poziomów usług wraz z powiązanymi karami lub mechanizmami obniżenia opłat za usługi mogą zostać zaproponowane jako dozwolona jednostronna zmiana zgodnie z klauzulą 1.1.3.

i) zasad ustalania cen lub innych przepisów finansowych,

Zmiana uzgodnionych opłat może zostać zaproponowana jako dozwolona jednostronna zmiana zgodnie z klauzulą 1.1.3, ale same zasady leżące u podstaw tych opłat – takie jak metodyka indeksacji cen – muszą zostać wspólnie uzgodnione przez strony.

j) miejsca przetwarzania lub przechowywania danych, jeżeli znajduje się ono poza UE.

Zmiany między miejscami w UE mogą zostać uzgodnione przez strony od początku ich stosunku umownego lub zaproponowane przez dostawcę jako dozwolona jednostronna zmiana. Jeżeli jednak miejsce przetwarzania lub przechowywania danych zmienia się z lokalizacji w UE na lokalizację poza UE lub z lokalizacji poza UE na inną lokalizację poza UE, strony muszą wzajemnie uzgodnić taką zmianę.

1.1.5. W przypadku zaproponowania dozwolonej jednostronnej zmiany dostawca musi:

a) powiadomić klienta nie później niż 30 dni kalendarzowych przed dniem, w którym proponowana dozwolona jednostronna zmiana stanie się skuteczna, chyba że prawo właściwe wymaga inaczej,

b) przekazać klientowi w jasny i zrozumiały sposób informacje obejmujące:

(i) zakres, szczegóły i harmonogram proponowanej dozwolonej jednostronnej zmiany,

(ii) uzasadnienie potrzeby wprowadzenia proponowanej dozwolonej jednostronnej zmiany, w tym w odniesieniu do płynących z niej korzyści dla klienta usług przetwarzania danych,

(iii) różnicę między stanem dotychczasowym a sytuacją po wprowadzeniu proponowanej dozwolonej jednostronnej zmiany. Obejmuje to w szczególności wszelkie ewentualne konsekwencje umowne, finansowe, organizacyjne, operacyjne, dotyczące poziomu świadczenia usług oraz zgodności z prawem dla klienta,

Opis takiej różnicy powinien odnosić się do przewidywanej sytuacji w odniesieniu do odpowiednich rodzajów istniejących klientów, z uwzględnieniem kategorii wskazanych w klauzuli 1.1.5 lit. b) pkt (iii). Ma to na celu zapewnienie, aby najbardziej prawdopodobne skutki zgłoszonej jednostronnej zmiany były widoczne i zrozumiałe dla klienta. W tym względzie klauzula ta nie wymaga od dostawcy zawiadamiania o ocenach dostosowanych do indywidualnych klientów.

(iv) planowany harmonogram wdrożenia i implementacji oraz datę wejścia w życie proponowanej dozwolonej jednostronnej zmiany.

1.1.6. Jeżeli dostawca spełnia warunki określone w klauzuli 1.1.5, uznaje się, że klient przyjął proponowaną dozwoloną jednostronną zmianę z dniem jej wejścia w życie.

1.1.7. Jeżeli dostawca narusza klauzule od 1.1.2 do 1.1.5 w odniesieniu do zmiany umowy, klient ma prawo rozwiązać umowę bez dodatkowych kosztów i uzyskać rekompensatę za poniesioną szkodę (z uwzględnieniem kosztów zmiany dostawcy usług przetwarzania danych). Nie ma to wpływu na inne prawa i środki ochrony prawnej klienta, w tym na prawo do wystąpienia o wydanie nakazu sądowego do dowolnego właściwego sądu w celu zobowiązania dostawcy do dalszego świadczenia usług zgodnie z umową, oraz do dochodzenia odszkodowania, jeżeli jest ono należne.

Jeżeli zmiana umowy przez dostawcę nie jest zgodna z postanowieniami umownymi, klient powinien mieć prawo do rozwiązania umowy, co w praktyce powinno również oznaczać złożenie zawiadomienia o zmianie dostawcy w celu wszczęcia procesu zmiany dostawcy (zob. standardowe postanowienia umowne dotyczące zmiany dostawcy i odejścia klienta – wariant A, jeżeli strony uzgodniły plan zmiany dostawcy i odejścia klienta, oraz wariant B w przypadku zautomatyzowanych narzędzi do samodzielnej zmiany dostawcy). W takich przypadkach klient powinien być jednak uprawniony do uzyskania odszkodowania za szkody poniesione w wyniku „przymusowej" zmiany dostawcy, w tym za poniesione koszty i inne związane z tym szkody (zob. standardowe postanowienia umowne dotyczące odpowiedzialności).

1.2. **Zawiadomienia**

Strony uzgadniają, że wszelkie zawiadomienia między nimi w odniesieniu do klauzul dotyczących niewprowadzania zmian będą dokonywane (*strony wskazują wybrane środki komunikacji, z uwzględnieniem odpowiednich środków elektronicznych*).

1.3. **Pierwszeństwo**

W przypadku jakiejkolwiek sprzeczności lub niespójności między niniejszymi klauzulami dotyczącymi niewprowadzania zmian a innymi mającymi zastosowanie ustaleniami umownymi, postanowieniami, warunkami lub innymi umowami odnoszącymi się do zmian umowy w zakresie objętym niniejszymi klauzulami pierwszeństwo mają niniejsze klauzule.

ZAŁĄCZNIK XII

STANDARDOWE POSTANOWIENIA UMOWNE

Definicje

Do celów standardowych postanowień umownych stosowane terminy definiuje się w następujący sposób:

„umowa" oznacza pisemną umowę między stronami dotyczącą świadczenia usług, wszelkie jej zmiany lub uzupełnienia, a także wszystkie akty związane z wykonaniem umowy lub umów, w tym w szczególności dodatki do umowy;

„dodatek" oznacza dodatek, harmonogram lub wykaz wyraźnie wymieniony w umowie;

„klient usług przetwarzania danych (klient)" oznacza, zgodnie z definicją w art. 2 pkt 30 aktu w sprawie danych, osobę fizyczną lub prawną, która nawiązała stosunek umowny z dostawcą usług przetwarzania danych w celu skorzystania z co najmniej jednej usługi przetwarzania danych;

„dane" oznaczają, zgodnie z definicją w art. 2 pkt 1 aktu w sprawie danych, wszelkie cyfrowe odwzorowania działań, faktów lub informacji oraz wszelkie kompilacje takich działań, faktów lub informacji, w tym w formie zapisu dźwiękowego, wizualnego lub audiowizualnego;

„akt w sprawie danych" oznacza rozporządzenie (UE) 2023/2854;

„opłaty z tytułu wychodzącego ruchu danych" oznaczają, zgodnie z definicją w art. 2 pkt 35 aktu w sprawie danych, opłaty za przekazanie danych pobierane od klientów za ekstrakcję ich danych przez sieć z infrastruktury ICT dostawcy usług przetwarzania danych do systemów innego dostawcy lub do lokalnej infrastruktury ICT;

„usługa przetwarzania danych" zdefiniowana w art. 2 pkt 8 aktu w sprawie danych oznacza świadczoną na rzecz klienta usługę cyfrową umożliwiającą wszechobecny sieciowy dostęp na żądanie do wspólnego zbioru konfigurowalnych, skalowalnych i elastycznych zasobów obliczeniowych o charakterze scentralizowanym, rozproszonym lub wysoce rozproszonym, które mogą być szybko przydzielone i uwolnione przy minimalnym wysiłku pod względem zarządzania lub interakcji z dostawcą usług. Do celów niniejszej umowy wspomniane usługi przetwarzania danych odnoszą się do usług świadczonych lub które mają być świadczone przez dostawcę na rzecz klienta, jak uzgodniono w umowie;

„docelowy dostawca", o którym mowa w art. 2 pkt 34 aktu w sprawie danych, oznacza docelowego dostawcę usług przetwarzania danych, do którego klient usługi przetwarzania danych przechodzi w celu korzystania z innej usługi przetwarzania danych usługi tego samego typu lub z innych usług;

„wyjściowy dostawca usług przetwarzania danych", o którym mowa w art. 2 pkt 34 aktu w sprawie danych, oznacza podmiot prawny, z którym klient nawiązał stosunek umowny dotyczący świadczenia usług przetwarzania danych i innych usług przez dostawcę na podstawie umowy i od którego klient zamierza obecnie przejść do innego dostawcy;

„aktywa cyfrowe" oznaczają, zgodnie z definicją w art. 2 pkt 32 aktu w sprawie danych, 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;

„dane eksportowalne" oznaczają, zgodnie z definicją w art. 2 pkt 38 aktu w sprawie danych, dane wejściowe i wyjściowe, w tym metadane, bezpośrednio lub pośrednio wygenerowane bądź współwygenerowane w wyniku korzystania przez klienta z usługi przetwarzania danych zapewnianej przez dostawców usług przetwarzania danych lub osoby trzecie, z wyłączeniem wszelkich aktywów lub danych, które są objęte prawami własności intelektualnej lub są tajemnicami przedsiębiorstwa;

„incydent" oznacza fizyczne, techniczne lub organizacyjne naruszenie bezpieczeństwa, incydent lub podobne zdarzenie, które może mieć znaczący wpływ na bezpieczeństwo i ciągłość działania, ponieważ spowodowało lub może spowodować poważne zakłócenie wszelkich mających zastosowanie systemów IT i operacji wykorzystywanych między dostawcą a klientem podczas procesu zmiany dostawcy lub w odniesieniu do korzystania przez klienta z usług, danych eksportowalnych i aktywów cyfrowych klienta. Zob. standardowe postanowienia umowne dotyczące bezpieczeństwa i ciągłości działania;

„interoperacyjność” oznacza, zgodnie z definicją w art. 2 pkt 40 aktu w sprawie danych, zdolność co najmniej dwóch przestrzeni danych lub sieci komunikacyjnych, systemów, produktów skomunikowanych, aplikacji, usług przetwarzania danych lub komponentów do wymiany i wykorzystywania danych w celu wykonywania swoich funkcji;

„metadane” oznaczają, zgodnie z definicją w art. 2 pkt 2 aktu w sprawie danych, ustrukturyzowany opis treści danych lub sposobu wykorzystywania danych, który ułatwia wyszukiwanie lub wykorzystywanie tych danych;

„dane nieosobowe” oznaczają, zgodnie z definicją w art. 2 pkt 4 aktu w sprawie danych: dane inne niż dane osobowe;

„lokalna infrastruktura ICT” oznacza, zgodnie z definicją w art. 2 pkt 33 aktu w sprawie danych, infrastrukturę ICT i zasoby obliczeniowe będące własnością klienta, przedmiotem najmu, dzierżawy lub leasingu przez niego, znajdujące się w jego własnym centrum danych i obsługiwane przez tego klienta lub osobę trzecią;

„inne usługi” oznaczają wszelkie profesjonalne usługi, niezależnie od ich charakteru, świadczone przez dostawcę na rzecz klienta na podstawie umowy zgodnie z definicją w niej zawartą, które nie są usługami przetwarzania danych;

„strona” oznacza klienta albo dostawcę;

„strony” oznaczają zarówno klienta, jak i dostawcę;

„dane osobowe” – zgodnie z definicją w art. 4 pkt 1 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych – „RODO”);

„plan” oznacza plan zmiany dostawcy i odejścia klienta, o którym mowa w standardowych postanowieniach umownych dotyczących planu zmiany dostawcy i odejścia klienta – wariant A, uzgodniony między stronami na mocy umowy;

„przetwarzanie” oznacza, zgodnie z definicją w art. 2 pkt 7 aktu w sprawie danych, operację lub zestaw operacji wykonywanych na danych lub zestawach danych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

„dostawca usług przetwarzania danych (dostawca)” oznacza osobę fizyczną lub prawną, która nawiązała stosunek umowny z klientem w celu świadczenia co najmniej jednej usługi przetwarzania danych;

„usługa tego samego typu” oznacza, zgodnie z definicją w art. 2 pkt 9 aktu w sprawie danych, zestaw usług przetwarzania danych, które mają ten sam główny cel, opierają się na tym samym modelu usługi przetwarzania danych i mają te same najważniejsze funkcje;

„usługi” oznaczają zarówno usługi przetwarzania danych, jak i wszystkie inne usługi uzgodnione przez strony na mocy umowy;

„opłata za usługę” oznacza opłaty należne i wymagalne od klienta na rzecz dostawcy jako wynagrodzenie za świadczenie usług uzgodnione przez strony na mocy umowy;

„zmiana dostawcy” oznacza, zgodnie z definicją w art. 2 pkt 34 aktu w sprawie danych, proces, w którym uczestniczą wyjściowy dostawca usług przetwarzania danych, klient korzystający z usługi przetwarzania danych oraz, w odpowiednich przypadkach, docelowy dostawca usług przetwarzania danych i w ramach którego klient korzystający z usługi przetwarzania danych przechodzi od korzystania z jednej usługi przetwarzania danych do korzystania z innej usługi tego samego typu lub z innej usługi oferowanych przez innego dostawcę usług przetwarzania danych, lub z lokalnej infrastruktury ICT, w tym poprzez ekstrakcję, transformację i załadowanie danych;

„opłaty z tytułu zmiany dostawcy” oznaczają, zgodnie z definicją w art. 2 pkt 36 aktu w sprawie danych, opłaty – inne niż standardowe opłaty za usługę lub kary za wcześniejsze rozwiązanie umowy – nakładane przez dostawcę usług przetwarzania danych na klienta za działania wymagane zgodnie z aktem w sprawie danych w celu zmiany na system innego dostawcy lub lokalną infrastrukturę ICT, w tym opłaty z tytułu wychodzącego ruchu danych.