WZÓR / TEMPLATE Wzór do dostosowania przed zawarciem umowy

Uwaga: niniejszy dokument jest wzorem udostępnianym przez WMK Invest sp. z o.o. w celu ułatwienia uzgodnienia umowy powierzenia z klientami. Przed zawarciem wzór należy dostosować do konkretnej współpracy: uzupełnić pola oznaczone [NAWIASAMI KWADRATOWYMI], wypełnić Załączniki nr 1–3, a zbędne warianty usunąć. Wzór nie stanowi porady prawnej. Postanowienia oznaczone jako „do negocjacji" mogą zostać zmienione w drodze uzgodnień Stron.

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta na podstawie art. 28 ust. 3 rozporządzenia (UE) 2016/679 (RODO)

zawarta w dniu [DATA] w [MIEJSCOWOŚĆ] albo — w przypadku zawarcia w formie elektronicznej — z dniem złożenia ostatniego kwalifikowanego podpisu elektronicznego (dalej: „**Umowa**"), pomiędzy:

[PEŁNA NAZWA (FIRMA) ADMINISTRATORA] z siedzibą w [MIEJSCOWOŚĆ], adres: [ADRES], wpisaną do [rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez SĄD, WYDZIAŁ, pod numerem KRS [NUMER] / Centralnej Ewidencji i Informacji o Działalności Gospodarczej], NIP [NIP], REGON [REGON], [kapitał zakładowy [KWOTA] zł — jeżeli dotyczy], reprezentowaną przez [IMIĘ I NAZWISKO — FUNKCJA / PODSTAWA UMOCOWANIA], zwaną dalej „**Administratorem**",

a

WMK Invest spółką z ograniczoną odpowiedzialnością z siedzibą w Katowicach, adres: ul. św. Jana 20, 40-012 Katowice, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Katowice-Wschód w Katowicach, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000520971, NIP 634-282-94-08, REGON 243619493, kapitał zakładowy 5 000,00 zł, reprezentowaną przez [IMIĘ I NAZWISKO — FUNKCJA], zwaną dalej „**Podmiotem przetwarzającym**",

zwanymi dalej łącznie „**Stronami**", a każda z osobna „**Stroną**".

Preambuła

Zważywszy, że:

1) Strony zawarły [NAZWA I DATA UMOWY GŁÓWNEJ] (dalej: „**Umowa Główna**"), na podstawie której Podmiot przetwarzający świadczy na rzecz Administratora usługi z zakresu wytwarzania oprogramowania, bezpieczeństwa IT, DevOps, integracji rozwiązań sztucznej inteligencji lub wsparcia technicznego;
2) wykonywanie Umowy Głównej wiąże się lub może wiązać się z przetwarzaniem przez Podmiot przetwarzający danych osobowych w imieniu Administratora;
3) Strony zamierzają uregulować zasady tego przetwarzania w sposób zapewniający zgodność z art. 28 RODO oraz właściwą ochronę praw osób, których dane dotyczą,

Strony postanawiają, co następuje:

§ 1. Definicje

1. Ilekroć w Umowie jest mowa o:
   1) **RODO** — należy przez to rozumieć 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);
   2) **Ustawie** — należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;

3) **Umowie Głównej** — należy przez to rozumieć umowę wskazaną w pkt 1 Preambuły, wraz z zamówieniami, specyfikacjami prac (SOW) i aneksami zawartymi na jej podstawie;

4) **Usługach** — należy przez to rozumieć usługi świadczone przez Podmiot przetwarzający na rzecz Administratora na podstawie Umowy Głównej, w zakresie wskazanym w Załączniku nr 1;

5) **Danych osobowych** lub **Danych** — należy przez to rozumieć dane osobowe w rozumieniu art. 4 pkt 1 RODO, przetwarzane przez Podmiot przetwarzający w imieniu Administratora w związku z wykonywaniem Usług;

6) **Dalszym podmiocie przetwarzającym** — należy przez to rozumieć inny podmiot przetwarzający, z którego usług korzysta Podmiot przetwarzający w celu wykonania w imieniu Administratora konkretnych czynności przetwarzania, o którym mowa w art. 28 ust. 2 i 4 RODO;

7) **Udokumentowanym poleceniu** — należy przez to rozumieć polecenie Administratora dotyczące przetwarzania Danych, wydane w sposób określony w § 3 ust. 2 lub 3 Umowy;

8) **Środkach bezpieczeństwa** — należy przez to rozumieć techniczne i organizacyjne środki ochrony Danych, o których mowa w art. 32 RODO, określone w szczególności w Załączniku nr 2;

9) **Organie nadzorczym** — należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych lub inny organ nadzorczy właściwy w rozumieniu art. 4 pkt 21 i art. 55–56 RODO;

10) **EOG** — należy przez to rozumieć Europejski Obszar Gospodarczy;

11) **Dniu roboczym** — należy przez to rozumieć dzień od poniedziałku do piątku, z wyjątkiem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej.

2. Pojęcia „przetwarzanie", „administrator", „podmiot przetwarzający", „osoba, której dane dotyczą", „naruszenie ochrony danych osobowych", „pseudonimizacja", „szczególne kategorie danych osobowych" oraz „organizacja międzynarodowa" mają znaczenie nadane im w RODO, w szczególności w art. 4 i art. 9 RODO.

§ 2. Przedmiot Umowy i zakres powierzenia

1. Na zasadach określonych w Umowie Administrator powierza Podmiotowi przetwarzającemu przetwarzanie Danych osobowych w jego imieniu, a Podmiot przetwarzający zobowiązuje się przetwarzać je zgodnie z Umową, RODO oraz innymi powszechnie obowiązującymi przepisami prawa.

2. Przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj Danych osobowych oraz kategorie osób, których dane dotyczą (art. 28 ust. 3 zdanie pierwsze RODO), określa Załącznik nr 1 do Umowy.

3. Podmiot przetwarzający może przetwarzać Dane wyłącznie w zakresie i celu niezbędnym do wykonania Usług. Podmiot przetwarzający nie jest uprawniony do przetwarzania Danych w celach własnych ani w jakichkolwiek innych celach, w szczególności do trenowania, dostrajania (fine-tuningu) lub ulepszania modeli sztucznej inteligencji, analityki lub profilowania na własny rachunek, chyba że Administrator wyda w tym zakresie wyraźne Udokumentowane polecenie.

4. Administrator oświadcza, że jest administratorem Danych lub — jeżeli sam przetwarza Dane jako podmiot przetwarzający w imieniu innego administratora — że jest uprawniony do dalszego powierzenia ich przetwarzania Podmiotowi przetwarzającemu w zakresie określonym w Umowie.

5. Administrator odpowiada za to, że przetwarzanie Danych odbywa się na podstawie prawnej wynikającej z art. 6 oraz — w odpowiednim przypadku — art. 9 lub 10 RODO, oraz za wykonanie wobec osób, których dane dotyczą, obowiązków informacyjnych, o których mowa w art. 13 i 14 RODO.

6. Przetwarzanie Danych w ramach Umowy trwa przez okres obowiązywania Umowy Głównej, a po jego zakończeniu — do czasu usunięcia lub zwrotu Danych zgodnie z § 13.

§ 3. Przetwarzanie na udokumentowane polecenie Administratora

1. Podmiot przetwarzający przetwarza Dane osobowe wyłącznie na Udokumentowane polecenie Administratora — co dotyczy także przekazywania Danych do państwa trzeciego lub organizacji międzynarodowej — chyba że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny (art. 28 ust. 3 lit. a RODO).
2. Udokumentowane polecenia Administratora stanowią w chwili zawarcia Umowy: postanowienia Umowy wraz z Załącznikami oraz postanowienia Umowy Głównej w zakresie, w jakim określają sposób świadczenia Usług.
3. Dalsze polecenia Administrator wydaje w formie pisemnej, w formie elektronicznej lub w formie dokumentowej (w szczególności wiadomością e-mail lub za pośrednictwem systemu zgłoszeń [NAZWA SYSTEMU ZGŁOSZEŃ]), wyłącznie przez osoby wskazane w Załączniku nr 1 jako upoważnione do wydawania poleceń. Polecenie wydane ustnie lub telefonicznie wymaga niezwłocznego potwierdzenia w jednej z powyższych form. Podmiot przetwarzający przechowuje Udokumentowane polecenia przez okres obowiązywania Umowy oraz przez okres przedawnienia roszczeń z niej wynikających.
4. Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych (art. 28 ust. 3 akapit drugi RODO). Do czasu potwierdzenia, zmiany lub wycofania takiego polecenia przez Administratora Podmiot przetwarzający może wstrzymać jego wykonanie, o czym informuje Administratora.
5. Wykonanie Udokumentowanych poleceń wykraczających poza zakres Usług lub Środków bezpieczeństwa uzgodnionych w Umowie może podlegać odrębnemu wynagrodzeniu na zasadach określonych w Umowie Głównej. Postanowienie zdania pierwszego nie dotyczy wykonywania obowiązków nałożonych na Podmiot przetwarzający bezpośrednio przez RODO.

§ 4. Poufność

1. Podmiot przetwarzający zapewnia, aby osoby upoważnione do przetwarzania Danych osobowych zobowiązały się do zachowania tajemnicy lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy (art. 28 ust. 3 lit. b RODO).
2. Podmiot przetwarzający dopuszcza do przetwarzania Danych wyłącznie osoby, które: posiadają imienne upoważnienie, o którym mowa w art. 29 i art. 32 ust. 4 RODO; zostały przeszkolone w zakresie ochrony danych osobowych i bezpieczeństwa informacji; przetwarzają Dane wyłącznie na polecenie Podmiotu przetwarzającego, wynikające z Udokumentowanych poleceń Administratora.
3. Podmiot przetwarzający prowadzi ewidencję osób upoważnionych do przetwarzania Danych i udostępnia ją Administratorowi na jego żądanie.
4. Obowiązek zachowania poufności trwa także po ustaniu zatrudnienia lub współpracy danej osoby z Podmiotem przetwarzającym oraz po rozwiązaniu lub wygaśnięciu Umowy, bez ograniczenia w czasie.
5. Poufnością objęte są również informacje o zabezpieczeniach systemów Administratora, w szczególności dane uwierzytelniające, klucze kryptograficzne, architektura systemów oraz podatności zidentyfikowane w toku audytów i testów bezpieczeństwa.

§ 5. Bezpieczeństwo przetwarzania

1. Podmiot przetwarzający podejmuje wszelkie środki wymagane na mocy art. 32 RODO (art. 28 ust. 3 lit. c RODO), uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

2. Minimalny zakres Środków bezpieczeństwa stosowanych przez Podmiot przetwarzający określa Załącznik nr 2. Podmiot przetwarzający regularnie testuje, mierzy i ocenia skuteczność Środków bezpieczeństwa (art. 32 ust. 1 lit. d RODO).
3. Podmiot przetwarzający może zmieniać Środki bezpieczeństwa w sposób odpowiadający rozwojowi technologii i zmianom ryzyka, pod warunkiem że zmiana nie obniży poziomu ochrony Danych. O istotnych zmianach Podmiot przetwarzający informuje Administratora w formie dokumentowej.
4. W zakresie, w jakim Podmiot przetwarzający przetwarza Dane w systemach, infrastrukturze lub kontach chmurowych Administratora, stosuje się do polityk bezpieczeństwa Administratora przekazanych mu w formie dokumentowej, a Administrator odpowiada za bezpieczeństwo tych elementów infrastruktury, które pozostają pod jego kontrolą.
5. Środowiska deweloperskie i testowe zasilane są danymi syntetycznymi, zanonimizowanymi lub spseudonimizowanymi. Wykorzystanie rzeczywistych Danych osobowych w tych środowiskach jest dopuszczalne wyłącznie na Udokumentowane polecenie Administratora i przy zastosowaniu Środków bezpieczeństwa odpowiadających środowisku produkcyjnemu.
6. W przypadku audytów bezpieczeństwa i testów penetracyjnych Podmiot przetwarzający przetwarza Dane, do których uzyska dostęp w toku testów, wyłącznie w zakresie niezbędnym do wykazania podatności; nie kopiuje Danych ponad niezbędne minimum dowodowe, a w raportach stosuje maskowanie lub pseudonimizację Danych.

§ 6. Dalsze powierzenie przetwarzania

1. Administrator udziela Podmiotowi przetwarzającemu uprzedniej ogólnej pisemnej zgody na korzystanie z usług Dalszych podmiotów przetwarzających (art. 28 ust. 2 oraz ust. 3 lit. d RODO). Dalsze podmioty przetwarzające wskazane w Załączniku nr 3 uważa się za zaakceptowane przez Administratora z chwilą zawarcia Umowy.
2. Podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia Dalszych podmiotów przetwarzających z wyprzedzeniem co najmniej [LICZBA] dni, w formie dokumentowej, na adres wskazany w Załączniku nr 1. Informacja obejmuje co najmniej: nazwę i siedzibę podmiotu, zakres powierzonych czynności, kategorie Danych, miejsce przetwarzania oraz — w razie przekazywania Danych poza EOG — podstawę prawną przekazania.
3. Administrator może, w terminie [LICZBA] dni od otrzymania informacji, o której mowa w ust. 2, wyrazić sprzeciw wobec zamierzonej zmiany, wskazując uzasadnione przyczyny związane z ochroną Danych. W takim przypadku Strony w dobrej wierze poszukują rozwiązania; jeżeli w terminie [LICZBA] dni od zgłoszenia sprzeciwu Strony nie dojdą do porozumienia, Podmiot przetwarzający nie powierzy Danych Administratora temu podmiotowi, a jeżeli nie jest to możliwe bez istotnego utrudnienia świadczenia Usług — Administrator może wypowiedzieć Umowę oraz Umowę Główną w zakresie Usług, których dotyczy zmiana, ze skutkiem natychmiastowym i bez obowiązku zapłaty kar umownych lub odszkodowania. [DO NEGOCJACJI]
4. Brak sprzeciwu w terminie, o którym mowa w ust. 3, oznacza akceptację zmiany.
5. Podmiot przetwarzający nakłada na Dalszy podmiot przetwarzający, w drodze umowy lub innego aktu prawnego podlegającego prawu Unii lub prawu państwa członkowskiego, te same obowiązki ochrony danych, jakie określono w Umowie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO (art. 28 ust. 4 RODO).
6. Jeżeli Dalszy podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego Dalszego podmiotu przetwarzającego spoczywa na Podmiocie przetwarzającym (art. 28 ust. 4 zdanie drugie RODO).
7. Na żądanie Administratora Podmiot przetwarzający udostępnia mu kopię postanowień umowy z Dalszym podmiotem przetwarzającym dotyczących ochrony danych; informacje stanowiące tajemnicę

przedsiębiorstwa mogą zostać zanonimizowane. Jeżeli Dalszy podmiot przetwarzający stosuje standardowe warunki umowne, wystarczające jest wskazanie miejsca ich publikacji.

§ 7. Pomoc w realizacji praw osób, których dane dotyczą

1. Biorąc pod uwagę charakter przetwarzania, Podmiot przetwarzający w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO (art. 28 ust. 3 lit. e RODO), w szczególności prawa dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych i sprzeciwu (art. 15–22 RODO).
2. Jeżeli osoba, której dane dotyczą, zwróci się z żądaniem bezpośrednio do Podmiotu przetwarzającego, Podmiot przetwarzający niezwłocznie, nie później niż w terminie [LICZBA] Dni roboczych, przekazuje żądanie Administratorowi i nie udziela odpowiedzi co do istoty sprawy bez Udokumentowanego polecenia Administratora; może jedynie poinformować tę osobę o przekazaniu żądania Administratorowi.
3. Na Udokumentowane polecenie Administratora Podmiot przetwarzający, w terminie [LICZBA] Dni roboczych, wykonuje operacje niezbędne do realizacji żądania, w szczególności sprostowanie, usunięcie lub ograniczenie przetwarzania Danych albo ich eksport w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.

§ 8. Pomoc w wywiązywaniu się z obowiązków określonych w art. 32–36 RODO

1. Uwzględniając charakter przetwarzania oraz dostępne mu informacje, Podmiot przetwarzający pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO (art. 28 ust. 3 lit. f RODO), w szczególności w zakresie:
   1) zapewnienia bezpieczeństwa przetwarzania (art. 32 RODO);
   2) zgłaszania naruszeń ochrony danych osobowych Organowi nadzorczemu oraz zawiadamiania o nich osób, których dane dotyczą (art. 33 i 34 RODO), na zasadach określonych w § 9;
   3) przeprowadzania oceny skutków dla ochrony danych (art. 35 RODO), w tym przez przekazanie opisu operacji przetwarzania, stosowanych Środków bezpieczeństwa i zidentyfikowanych ryzyk w terminie [LICZBA] Dni roboczych od otrzymania żądania;
   4) uprzednich konsultacji z Organem nadzorczym (art. 36 RODO).
2. Postanowienie § 3 ust. 5 stosuje się odpowiednio do pomocy wykraczającej poza obowiązki wynikające bezpośrednio z RODO.

§ 9. Naruszenia ochrony danych osobowych

1. Po stwierdzeniu naruszenia ochrony danych osobowych dotyczącego Danych Podmiot przetwarzający bez zbędnej zwłoki, nie później niż w ciągu [LICZBA, np. 24 lub 36] godzin od stwierdzenia naruszenia, zgłasza je Administratorowi (art. 33 ust. 2 RODO).
2. Zgłoszenia dokonuje się na adres e-mail i numer telefonu Administratora wskazane w Załączniku nr 1 jako kontakt w sprawie naruszeń.
3. Zgłoszenie zawiera co najmniej informacje, o których mowa w art. 33 ust. 3 RODO, tj.:
   a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie;
   b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opis możliwych konsekwencji naruszenia ochrony danych osobowych;

d) opis środków zastosowanych lub proponowanych przez Podmiot przetwarzający w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków;

e) ponadto — w miarę dostępności — czas wystąpienia i stwierdzenia naruszenia oraz wskazanie systemów, których naruszenie dotyczy.

4. Jeżeli — i w zakresie, w jakim — informacji nie da się udzielić w tym samym czasie, Podmiot przetwarzający może ich udzielać sukcesywnie, bez zbędnej dalszej zwłoki (art. 33 ust. 4 RODO).

5. Podmiot przetwarzający niezwłocznie podejmuje działania w celu ograniczenia skutków naruszenia, zabezpiecza dowody, dokumentuje naruszenie oraz współpracuje z Administratorem przy jego wyjaśnianiu, zgłoszeniu Organowi nadzorczemu i zawiadomieniu osób, których dane dotyczą.

6. Podmiot przetwarzający nie zgłasza naruszenia Organowi nadzorczemu ani nie zawiadamia o nim osób, których dane dotyczą, w imieniu Administratora, chyba że Administrator wyda takie Udokumentowane polecenie albo obowiązek taki wynika z przepisów prawa.

§ 10. Udostępnianie informacji i audyty

1. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz w Umowie, a także umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich (art. 28 ust. 3 lit. h RODO). Postanowienie § 3 ust. 4 stosuje się.

2. Administrator zawiadamia Podmiot przetwarzający o zamiarze przeprowadzenia audytu z wyprzedzeniem co najmniej [LICZBA] Dni roboczych, w formie dokumentowej, wskazując planowany termin, zakres oraz osoby przeprowadzające audyt. W przypadku naruszenia ochrony Danych, uzasadnionego podejrzenia naruszenia Umowy lub żądania Organu nadzorczego termin ten wynosi [LICZBA] Dni roboczych.

3. Audytor zewnętrzny, przed przystąpieniem do audytu, zobowiązuje się wobec Podmiotu przetwarzającego na piśmie lub w formie elektronicznej do zachowania poufności. Podmiot przetwarzający może zgłosić uzasadniony sprzeciw wobec audytora będącego jego bezpośrednim konkurentem; w takim przypadku Administrator wskaże innego audytora.

4. Audyt przeprowadza się w Dni robocze, w godzinach pracy Podmiotu przetwarzającego, w sposób nieutrudniający w nadmierny sposób jego działalności oraz bez dostępu do danych innych klientów i tajemnic przedsiębiorstwa Podmiotu przetwarzającego niezwiązanych z przetwarzaniem Danych. Testy techniczne (w tym testy penetracyjne) infrastruktury Podmiotu przetwarzającego wymagają uprzedniego uzgodnienia ich zakresu i zasad.

5. Bez uszczerbku dla prawa Administratora do przeprowadzenia audytu, w tym inspekcji, Podmiot przetwarzający może w pierwszej kolejności udostępnić dokumentację potwierdzającą zgodność, w szczególności wypełnione kwestionariusze bezpieczeństwa, polityki i procedury, raporty z audytów lub testów oraz [CERTYFIKATY / RAPORTY NIEZALEŻNYCH AUDYTORÓW — JEŻELI DOTYCZY].

6. Audyty przeprowadza się nie częściej niż raz na 12 miesięcy, z wyjątkiem audytów związanych z naruszeniem ochrony Danych, uzasadnionym podejrzeniem naruszenia Umowy lub żądaniem Organu nadzorczego.

7. Każda ze Stron ponosi własne koszty związane z audytem; koszty audytora zewnętrznego ponosi Administrator. Czas pracy personelu Podmiotu przetwarzającego przekraczający [LICZBA] godzin na jeden audyt może zostać rozliczony według stawek określonych w Umowie Głównej, chyba że audyt wykaże istotne naruszenie Umowy przez Podmiot przetwarzający — wówczas Podmiot przetwarzający ponosi uzasadnione koszty audytu. [DO NEGOCJACJI]

8. Z audytu sporządza się protokół. Podmiot przetwarzający usuwa stwierdzone nieprawidłowości w terminie uzgodnionym przez Strony, nie dłuższym niż [LICZBA] dni od otrzymania protokołu.

§ 11. Rejestr czynności przetwarzania i współpraca z Organem nadzorczym

1. Podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zawierający informacje, o których mowa w art. 30 ust. 2 RODO, tj.:
   a) imię i nazwisko lub nazwę oraz dane kontaktowe Podmiotu przetwarzającego, Administratora oraz — gdy ma to zastosowanie — przedstawiciela Administratora lub Podmiotu przetwarzającego oraz inspektora ochrony danych;
   b) kategorie przetwarzań dokonywanych w imieniu Administratora;
   c) gdy ma to zastosowanie — przekazania Danych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń;
   d) jeżeli jest to możliwe — ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
2. Podmiot przetwarzający udostępnia rejestr Organowi nadzorczemu na jego żądanie (art. 30 ust. 4 RODO).
3. Podmiot przetwarzający współpracuje z Organem nadzorczym, w szczególności z Prezesem Urzędu Ochrony Danych Osobowych, w ramach wykonywania jego zadań (art. 31 RODO).
4. Podmiot przetwarzający niezwłocznie informuje Administratora o: wszczęciu wobec niego kontroli lub postępowania przez Organ nadzorczy w zakresie dotyczącym Danych; żądaniach udostępnienia Danych kierowanych do niego przez organy publiczne — o ile przepisy prawa nie zabraniają przekazania takiej informacji; a także o postępowaniach sądowych lub administracyjnych dotyczących przetwarzania Danych.
5. Dane kontaktowe Podmiotu przetwarzającego w sprawach ochrony danych osobowych (oraz inspektora ochrony danych — jeżeli został wyznaczony) wskazuje Załącznik nr 1.

§ 12. Przekazywanie Danych poza EOG

1. Podmiot przetwarzający przetwarza Dane na terytorium EOG, chyba że Administrator wyrazi uprzednią zgodę w formie dokumentowej na przekazanie Danych do państwa trzeciego lub organizacji międzynarodowej, w szczególności przez akceptację Dalszego podmiotu przetwarzającego wskazanego w Załączniku nr 3 z oznaczeniem miejsca przetwarzania poza EOG.
2. Przekazanie Danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie po spełnieniu warunków określonych w rozdziale V RODO, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony (art. 45 RODO) albo z zastosowaniem odpowiednich zabezpieczeń (art. 46 RODO), takich jak standardowe klauzule umowne przyjęte przez Komisję Europejską lub wiążące reguły korporacyjne (art. 47 RODO).
3. W przypadku stosowania standardowych klauzul umownych Podmiot przetwarzający zapewnia ich zawarcie z Dalszym podmiotem przetwarzającym we właściwym module, a w razie potrzeby — przeprowadzenie oceny skutków przekazania oraz wdrożenie środków uzupełniających (w szczególności szyfrowania).
4. Za przekazanie Danych poza EOG uważa się także zdalny dostęp do Danych z terytorium państwa trzeciego.
5. Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli podstawa przekazania przestanie zapewniać odpowiedni stopień ochrony Danych.

§ 13. Usunięcie lub zwrot Danych

1. Po zakończeniu świadczenia Usług związanych z przetwarzaniem Podmiot przetwarzający, zależnie od decyzji Administratora, usuwa lub zwraca mu wszelkie Dane osobowe oraz usuwa wszelkie ich istniejące

kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie Danych (art. 28 ust. 3 lit. g RODO).

2. Administrator wskazuje swój wybór w formie dokumentowej w terminie [LICZBA] dni od zakończenia świadczenia Usług. W braku wskazania w tym terminie Podmiot przetwarzający [usuwa Dane / zwraca Dane i usuwa ich kopie]. [DO NEGOCJACJI]
3. Zwrot Danych następuje w formacie [FORMAT, np. eksport bazy danych / CSV / JSON] lub innym uzgodnionym przez Strony, za pośrednictwem bezpiecznego kanału transmisji.
4. Podmiot przetwarzający usuwa Dane, w tym u Dalszych podmiotów przetwarzających, w terminie [LICZBA] dni od dokonania wyboru przez Administratora albo upływu terminu, o którym mowa w ust. 2. Dane znajdujące się w kopiach zapasowych są usuwane zgodnie z cyklem rotacji kopii, nie później niż w terminie [LICZBA] dni; do czasu usunięcia są one chronione zgodnie z Umową i nie są wykorzystywane w żadnym celu.
5. Podmiot przetwarzający potwierdza Administratorowi usunięcie lub zwrot Danych w formie dokumentowej, w terminie [LICZBA] dni od ich dokonania.
6. Jeżeli przepisy prawa nakazują dalsze przechowywanie Danych, Podmiot przetwarzający informuje Administratora o podstawie prawnej i okresie przechowywania, przetwarza Dane wyłącznie w celu wynikającym z tych przepisów oraz stosuje do nich postanowienia Umowy dotyczące poufności i bezpieczeństwa.

§ 14. Odpowiedzialność

1. Każda ze Stron odpowiada wobec osób, których dane dotyczą, na zasadach określonych w art. 82 RODO. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie wówczas, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem Udokumentowanymi poleceniami Administratora lub wbrew tym poleceniom (art. 82 ust. 2 RODO).
2. Strona jest zwolniona z odpowiedzialności, jeżeli udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody (art. 82 ust. 3 RODO).
3. Strona, która zapłaciła odszkodowanie za całą wyrządzoną szkodę, ma prawo żądać od drugiej Strony zwrotu części odszkodowania odpowiadającej części szkody, za którą ta Strona ponosi odpowiedzialność (art. 82 ust. 5 RODO).
4. Odpowiedzialność Podmiotu przetwarzającego wobec Administratora z tytułu niewykonania lub nienależytego wykonania Umowy podlega zasadom ogólnym Kodeksu cywilnego [oraz ograniczeniom odpowiedzialności przewidzianym w Umowie Głównej / jest ograniczona do kwoty [KWOTA] zł / jest ograniczona do [KROTNOŚĆ] wynagrodzenia netto zapłaconego na podstawie Umowy Głównej w okresie [LICZBA] miesięcy poprzedzających zdarzenie wywołujące szkodę]. Ograniczenie nie dotyczy szkody wyrządzonej umyślnie (art. 473 § 2 Kodeksu cywilnego). [DO NEGOCJACJI — WYBRAĆ WARIANT]
5. Podmiot przetwarzający nie ponosi odpowiedzialności za skutki wykonania Udokumentowanego polecenia Administratora, z zastrzeżeniem obowiązku, o którym mowa w § 3 ust. 4.

§ 15. Czas obowiązywania i rozwiązanie Umowy

1. Umowa zostaje zawarta na czas obowiązywania Umowy Głównej i wygasa wraz z jej rozwiązaniem lub wygaśnięciem, z zastrzeżeniem ust. 4.
2. Administrator może wypowiedzieć Umowę ze skutkiem natychmiastowym, jeżeli Podmiot przetwarzający:
   1) przetwarza Dane w sposób sprzeczny z Umową lub RODO i — mimo wezwania w formie dokumentowej — nie usunie naruszenia w terminie [LICZBA] dni od otrzymania wezwania;

2) przetwarza Dane w celu innym niż określony w Umowie;

3) uniemożliwia lub w sposób nieuzasadniony utrudnia przeprowadzenie audytu, o którym mowa w § 10;

4) zgodnie z prawomocnym orzeczeniem sądu lub ostateczną decyzją Organu nadzorczego nie zapewnia wystarczających gwarancji ochrony Danych.

3. Wypowiedzenie Umowy z przyczyn, o których mowa w ust. 2, uprawnia Administratora do wypowiedzenia Umowy Głównej w zakresie Usług wymagających przetwarzania Danych, ze skutkiem natychmiastowym.

4. Postanowienia § 4, § 10, § 11 ust. 4, § 13 i § 14 obowiązują także po rozwiązaniu lub wygaśnięciu Umowy — do czasu wykonania wynikających z nich obowiązków.

§ 16. Relacja do Umowy Głównej i pierwszeństwo postanowień

1. Umowa uzupełnia Umowę Główną. W sprawach nieuregulowanych w Umowie stosuje się postanowienia Umowy Głównej, RODO, Ustawy oraz Kodeksu cywilnego.

2. W razie sprzeczności między postanowieniami Umowy a postanowieniami Umowy Głównej lub innych umów łączących Strony w sprawach dotyczących ochrony danych osobowych pierwszeństwo mają postanowienia Umowy.

3. W razie sprzeczności między treścią Umowy a treścią Załączników pierwszeństwo ma treść Umowy, chyba że Załącznik przewiduje wyższy poziom ochrony Danych.

4. Z tytułu wykonywania Umowy Podmiotowi przetwarzającemu nie przysługuje odrębne wynagrodzenie ponad wynagrodzenie określone w Umowie Głównej, z zastrzeżeniem § 3 ust. 5, § 8 ust. 2 oraz § 10 ust. 7.

§ 17. Postanowienia końcowe

1. Umowa zostaje zawarta w formie pisemnej (art. 78 Kodeksu cywilnego) albo w formie elektronicznej przez złożenie przez każdą ze Stron kwalifikowanego podpisu elektronicznego (art. 78¹ Kodeksu cywilnego), co odpowiada wymogowi art. 28 ust. 9 RODO.

2. Zmiany Umowy wymagają formy pisemnej albo formy elektronicznej pod rygorem nieważności, z wyjątkiem: aktualizacji Załącznika nr 3 w trybie § 6, zmiany Środków bezpieczeństwa w trybie § 5 ust. 3 oraz zmiany danych kontaktowych wskazanych w Załączniku nr 1 — dla których wystarczająca jest forma dokumentowa.

3. Umowa podlega prawu polskiemu.

4. Spory wynikające z Umowy lub z nią związane rozstrzyga sąd powszechny właściwy miejscowo dla siedziby Podmiotu przetwarzającego. [DO NEGOCJACJI — ALTERNATYWNIE: SĄD WŁAŚCIWY WEDŁUG PRZEPISÓW OGÓLNYCH]

5. Jeżeli którekolwiek z postanowień Umowy okaże się nieważne lub bezskuteczne, pozostałe postanowienia pozostają w mocy, a Strony zastąpią postanowienie nieważne lub bezskuteczne postanowieniem ważnym, możliwie najbliższym jego celowi. Umowę interpretuje się w sposób zapewniający zgodność z RODO.

6. W razie zmiany przepisów prawa, wydania przez Komisję Europejską nowych standardowych klauzul umownych w rozumieniu art. 28 ust. 7 RODO lub wytycznych Europejskiej Rady Ochrony Danych, które wymagają dostosowania Umowy, Strony podejmą w dobrej wierze negocjacje w celu jej zmiany.

7. Umowa została sporządzona w języku polskim. Strony mogą posługiwać się tłumaczeniem Umowy na język angielski wyłącznie w celach informacyjnych; w razie rozbieżności rozstrzygające znaczenie ma wersja polska.

8. W przypadku zawarcia Umowy w formie pisemnej Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

9. Integralną część Umowy stanowią:

1) Załącznik nr 1 — Opis przetwarzania i dane kontaktowe;
2) Załącznik nr 2 — Techniczne i organizacyjne środki bezpieczeństwa;
3) Załącznik nr 3 — Wykaz Dalszych podmiotów przetwarzających.

Za Administratora

podpis

[IMIĘ I NAZWISKO — FUNKCJA]

Data: [DATA]

☐ podpis własnoręczny
☐ kwalifikowany podpis elektroniczny

Za Podmiot przetwarzający

podpis

[IMIĘ I NAZWISKO — FUNKCJA]

Data: [DATA]

☐ podpis własnoręczny
☐ kwalifikowany podpis elektroniczny

Załącznik nr 1 — Opis przetwarzania i dane kontaktowe

(art. 28 ust. 3 zdanie pierwsze RODO) — do uzupełnienia przez Strony; należy zaznaczyć właściwe pola i usunąć pozostałe.

A. Usługi, w ramach których następuje przetwarzanie

☐	Usługa	Typowy charakter czynności przetwarzania
☐	Wytwarzanie i rozwój oprogramowania	Dostęp do Danych w środowiskach deweloperskich, testowych i produkcyjnych w zakresie niezbędnym do wdrożeń, migracji danych, diagnozy i usuwania błędów.
☐	Hosting, utrzymanie i administracja systemów	Przechowywanie Danych, wykonywanie kopii zapasowych, administracja serwerami i bazami danych, monitorowanie dostępności.
☐	Usługi DevOps / SRE / chmura	Konfiguracja infrastruktury i potoków CI/CD, zarządzanie dostępami, zbieranie i analiza logów oraz metryk.
☐	Audyty bezpieczeństwa i testy penetracyjne	Incydentalny dostęp do Danych w testowanych systemach, przeglądanie, ograniczone utrwalanie dowodów podatności.
☐	Integracje rozwiązań AI (LLM, RAG, automatyzacja)	Przetwarzanie Danych w zapytaniach (promptach) i dokumentach, tworzenie indeksów wektorowych, przekazywanie Danych dostawcom modeli wskazanym w Załączniku nr 3.
☐	Wsparcie techniczne / helpdesk / SLA	Obsługa zgłoszeń, analiza logów i zrzutów ekranu, diagnoza błędów z udziałem Danych.
☐	Inne: [OPIS]	[OPIS]

B. Opis przetwarzania

Element	Opis (do uzupełnienia)
Przedmiot przetwarzania	Dane osobowe przetwarzane w związku ze świadczeniem Usług zaznaczonych w części A, w systemach: [NAZWY SYSTEMÓW / APLIKACJI / ŚRODOWISK].
Czas trwania przetwarzania	Okres obowiązywania Umowy Głównej [od [DATA] do [DATA] / na czas nieokreślony], a po jego zakończeniu — do czasu usunięcia lub zwrotu Danych zgodnie z § 13.
Charakter przetwarzania (operacje)	☐ zbieranie ☐ utrwalanie ☐ organizowanie ☐ porządkowanie ☐ przechowywanie ☐ adaptowanie lub modyfikowanie ☐ pobieranie ☐ przeglądanie ☐ wykorzystywanie ☐ ujawnianie przez przesłanie ☐ dopasowywanie lub łączenie ☐ ograniczanie ☐ usuwanie lub niszczenie ☐ inne: [OPIS]
Cel przetwarzania	Wykonanie Usług na rzecz Administratora zgodnie z Umową Główną, w szczególności: [OPIS CELU].

Element	Opis (do uzupełnienia)
Rodzaj danych osobowych	☐ dane identyfikacyjne (np. imię, nazwisko) ☐ dane kontaktowe (np. e-mail, telefon, adres) ☐ dane kont użytkowników (np. login, identyfikatory, skróty haseł) ☐ dane techniczne (np. adresy IP, identyfikatory urządzeń, logi, pliki cookies) ☐ dane transakcyjne i dotyczące zamówień ☐ dane dotyczące zatrudnienia ☐ treść komunikacji i zgłoszeń ☐ dane zawarte w dokumentach przetwarzanych przez rozwiązania AI ☐ inne: [OPIS]
Szczególne kategorie danych (art. 9 RODO) oraz dane dotyczące wyroków skazujących (art. 10 RODO)	☐ nie dotyczy ☐ dotyczy: [WSKAZAĆ KATEGORIE] — wymaga uzgodnienia dodatkowych Środków bezpieczeństwa.
Kategorie osób, których dane dotyczą	☐ klienci i użytkownicy końcowi Administratora ☐ pracownicy i współpracownicy Administratora ☐ kontrahenci Administratora i ich przedstawiciele ☐ kandydaci do pracy ☐ osoby kontaktujące się z Administratorem ☐ inne: [OPIS]
Szacunkowa skala przetwarzania	[LICZBA OSÓB / REKORDÓW]
Miejsce przetwarzania	☐ infrastruktura Administratora ☐ infrastruktura Podmiotu przetwarzającego ☐ infrastruktura Dalszych podmiotów przetwarzających (Załącznik nr 3); państwo / region: [WSKAZAĆ]
Częstotliwość przetwarzania	☐ ciągła ☐ okresowa ☐ incydentalna / jednorazowa

C. Dane kontaktowe

Rola	Administrator	Podmiot przetwarzający
Osoba odpowiedzialna za wykonanie Umowy	[IMIĘ I NAZWISKO, E-MAIL, TELEFON]	[IMIĘ I NAZWISKO, E-MAIL, TELEFON]
Osoby upoważnione do wydawania poleceń (§ 3 ust. 3)	[IMIĘ I NAZWISKO, E-MAIL]	nie dotyczy
Kontakt w sprawie naruszeń ochrony danych (§ 9)	[E-MAIL, TELEFON]	[E-MAIL, TELEFON]
Inspektor ochrony danych (jeżeli wyznaczony)	[IMIĘ I NAZWISKO, E-MAIL]	[IMIĘ I NAZWISKO, E-MAIL / nie wyznaczono]
Adres do zawiadomień o Dalszych podmiotach przetwarzających (§ 6)	[E-MAIL]	nie dotyczy

Załącznik nr 2 — Techniczne i organizacyjne środki bezpieczeństwa

(art. 28 ust. 3 lit. c i art. 32 RODO) — minimalny zakres środków stosowanych przez Podmiot przetwarzający.

Obszar	Środki
1. Zarządzanie bezpieczeństwem	Udokumentowana polityka bezpieczeństwa informacji i ochrony danych; wyznaczona osoba odpowiedzialna za bezpieczeństwo; analiza ryzyka przeprowadzana przed rozpoczęciem przetwarzania i aktualizowana co najmniej raz w roku.
2. Kontrola dostępu i tożsamość	Uwierzytelnianie wieloskładnikowe (MFA) do wszystkich systemów, w których przetwarzane są Dane (poczta, repozytoria kodu, konsole chmurowe, VPN, menedżer haseł). Zasada najmniejszych uprawnień i wiedzy koniecznej. Wyłącznie imienne konta — zakaz kont współdzielonych. Dostęp nadawany na czas realizacji projektu i odbierany po jego zakończeniu lub w ciągu [LICZBA] Dni roboczych od zmiany składu zespołu. Przegląd uprawnień co najmniej [CO KWARTAŁ]. Dostęp uprzywilejowany z wykorzystaniem odrębnych kont lub hosta pośredniczącego (bastion).
3. Szyfrowanie	Szyfrowanie transmisji (TLS 1.2 lub nowszy, SSH, VPN). Szyfrowanie danych w spoczynku: pełne szyfrowanie dysków wszystkich urządzeń końcowych, szyfrowanie baz danych, magazynów danych i kopii zapasowych (AES-256 lub równoważne). Zarządzanie sekretami w dedykowanym narzędziu; zakaz przechowywania sekretów w repozytoriach kodu.
4. Rejestrowanie zdarzeń i monitorowanie	Rejestrowanie dostępu do systemów i operacji administracyjnych; centralne gromadzenie logów; monitorowanie i alertowanie z wykorzystaniem systemu klasy SIEM; ochrona logów przed nieuprawnioną modyfikacją; przechowywanie logów przez [LICZBA] dni; synchronizacja czasu.
5. Kopie zapasowe i ciągłość działania	Regularne kopie zapasowe zgodnie z harmonogramem uzgodnionym w Umowie Głównej, szyfrowane i przechowywane w centrach danych na terytorium EOG; okresowe testy odtwarzania; zdolność do szybkiego przywrócenia dostępności Danych w razie incydentu (art. 32 ust. 1 lit. c RODO); parametry RPO/RTO: [WSKAZAĆ].
6. Zarządzanie podatnościami	Regularne skanowanie podatności systemów i zależności (SCA); instalowanie poprawek krytycznych w terminie [LICZBA] dni od ich udostępnienia; ochrona urządzeń końcowych (EDR / oprogramowanie antywirusowe); utwardzanie konfiguracji zgodnie z uznanymi standardami (np. CIS Benchmarks).
7. Bezpieczny cykl wytwarzania oprogramowania (Secure SDLC)	Przegląd kodu (code review); automatyczne testy bezpieczeństwa w potokach CI/CD (SAST, SCA, wykrywanie sekretów); separacja środowisk deweloperskich, testowych i produkcyjnych; zarządzanie zmianą; uwzględnianie wymagań bezpieczeństwa (np. OWASP Top 10 / ASVS); testy penetracyjne kluczowych aplikacji.
8. Minimalizacja danych w środowiskach testowych i rozwiązaniach AI	Wykorzystywanie danych syntetycznych, zanonimizowanych lub spseudonimizowanych w środowiskach deweloperskich i testowych; kopie danych produkcyjnych wyłącznie na Udokumentowane polecenie, z zabezpieczeniami jak dla produkcji i usunięciem po zakończeniu testów; maskowanie Danych w logach i raportach. W integracjach AI: przekazywanie Danych wyłącznie dostawcom wskazanym w Załączniku nr 3, wyłączenie wykorzystania Danych do trenowania modeli oraz konfiguracja ograniczonej retencji — o ile dostawca to umożliwia.
9. Zarządzanie incydentami	Udokumentowana procedura obsługi incydentów bezpieczeństwa (wykrycie, klasyfikacja, ograniczanie skutków, usuwanie przyczyn, analiza po incydencie); rejestr incydentów i naruszeń; zgłaszanie naruszeń Administratorowi w terminie określonym w § 9 ust. 1.
10. Personel i szkolenia	Pisemne zobowiązania do zachowania poufności; imienne upoważnienia do przetwarzania danych (art. 29 RODO); szkolenia z ochrony danych i bezpieczeństwa przy rozpoczęciu współpracy i co najmniej raz w roku, w tym w zakresie rozpoznawania phishingu; procedura zakończenia współpracy obejmująca niezwłoczne odebranie dostępów i zwrot sprzętu.

Obszar	Środki
11. Bezpieczeństwo fizyczne i urządzeń	Służbowe, zarządzane centralnie urządzenia z szyfrowaniem dysku, automatyczną blokadą ekranu i możliwością zdalnego wymazania danych; zakaz przetwarzania Danych na prywatnych urządzeniach niespełniających wymogów bezpieczeństwa; zasada czystego biurka i czystego ekranu; kontrola dostępu do pomieszczeń; bezpieczne niszczenie nośników (bezpieczne wymazywanie lub fizyczne zniszczenie).
12. Dalsze podmioty przetwarzające	Weryfikacja gwarancji ochrony danych przed powierzeniem; umowy spełniające wymogi art. 28 ust. 4 RODO; okresowy przegląd Dalszych podmiotów przetwarzających.
13. Pseudonimizacja i ocena skuteczności	Pseudonimizacja Danych tam, gdzie jest to możliwe (art. 32 ust. 1 lit. a RODO); regularne testowanie, mierzenie i ocena skuteczności środków, w tym przegląd niniejszego Załącznika co najmniej raz w roku (art. 32 ust. 1 lit. d RODO).
14. Środki dodatkowe uzgodnione z Administratorem	[OPIS — JEŻELI DOTYCZY]

Załącznik nr 3 — Wykaz Dalszych podmiotów przetwarzających

(art. 28 ust. 2 i 4 RODO) — wykaz zaakceptowany przez Administratora z chwilą zawarcia Umowy (§ 6 ust. 1).

☐ Na dzień zawarcia Umowy Podmiot przetwarzający nie korzysta z usług Dalszych podmiotów przetwarzających.

☐ Na dzień zawarcia Umowy Podmiot przetwarzający korzysta z usług następujących Dalszych podmiotów przetwarzających:

Lp.	Nazwa, siedziba i dane rejestrowe	Zakres czynności przetwarzania	Kategorie Danych	Miejsce przetwarzania	Podstawa przekazania poza EOG (jeżeli dotyczy)
1.	[NAZWA, ADRES]	[np. hosting / infrastruktura chmurowa]	[KATEGORIE]	[PAŃSTWO]	[np. art. 45 / art. 46 ust. 2 lit. c RODO]
2.	[NAZWA, ADRES]	[np. poczta elektroniczna i narzędzia biurowe]	[KATEGORIE]	[PAŃSTWO]	[PODSTAWA]
3.	[NAZWA, ADRES]	[np. dostawca modeli AI]	[KATEGORIE]	[PAŃSTWO]	[PODSTAWA]
4.	[NAZWA, ADRES]	[np. system zgłoszeń / repozytorium kodu]	[KATEGORIE]	[PAŃSTWO]	[PODSTAWA]
5.	[NAZWA, ADRES]	[ZAKRES]	[KATEGORIE]	[PAŃSTWO]	[PODSTAWA]

Zmiany niniejszego wykazu następują w trybie § 6 ust. 2–4 Umowy.