Umowa powierzenia przetwarzania danych osobowych (DPA)

zawarta w dniu ..... w ....., pomiędzy:

Marek Łobaza, z siedzibą w Warszawie, adres: ul. Jana Kazimierza 33A lok. 63, 01-248 Warszawa, NIP: 6861655065, REGON: 520777134,

reprezentowany przez Marka Łobazę, zwany dalej **„Procesorem"**,

a

Phinia (PHINIA DELPHI POLAND Spółka z ograniczoną odpowiedzialnością) z siedzibą w Warszawie, adres: ul. Jutrzenki 137A, 02-231 Warszawa, NIP: 6222781627, KRS: 0000434101,

reprezentowaną przez ....., zwaną dalej **„Administratorem"** / **„Klientem"**,

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

§ 1. Definicje

1. **RODO** – 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.
2. **Umowa główna** – umowa SaaS / Service Agreement zawarta pomiędzy Stronami, której niniejsza Umowa powierzenia stanowi załącznik.
3. **Dane osobowe** – dane osobowe w rozumieniu art. 4 pkt 1 RODO, przetwarzane przez Procesora w imieniu Administratora w związku z realizacją Umowy głównej.
4. **Przetwarzanie** – operacje przetwarzania danych osobowych opisane w Załączniku nr 1 („Opis przetwarzania danych").
5. **Subprocesor** – podmiot przetwarzający, któremu Procesor powierza przetwarzanie danych osobowych w imieniu Administratora.
6. **Naruszenie ochrony danych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 2. Przedmiot i czas trwania powierzenia

1. Niniejsza Umowa określa zasady powierzenia przetwarzania danych osobowych przez Administratora na rzecz Procesora w związku ze świadczeniem usług SaaS na podstawie Umowy głównej.
2. Przetwarzanie danych osobowych odbywa się przez cały okres obowiązywania Umowy głównej, a w zakresie określonym w § 13 – także po jej zakończeniu.
3. Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek przetwarzania wynika z bezwzględnie obowiązujących przepisów prawa – w takim przypadku Procesor informuje Administratora o tym obowiązku przed rozpoczęciem przetwarzania.

§ 3. Charakter i cel przetwarzania

1. Charakter przetwarzania: gromadzenie, przechowywanie, porządkowanie, przeglądanie, udostępnianie techniczne, modyfikowanie, ograniczanie, usuwanie oraz inne operacje niezbędne do świadczenia usługi SaaS.
2. Cel przetwarzania: świadczenie usługi SaaS na rzecz Administratora, w tym udostępnianie systemu, administrowanie środowiskiem, zapewnienie bezpieczeństwa, wsparcie techniczne, tworzenie kopii zapasowych oraz utrzymanie ciągłości działania.
3. Szczegółowy opis przedmiotu, celu, rodzajów danych oraz kategorii osób, których dane dotyczą, określa Załącznik nr 1.

§ 4. Rodzaje danych osobowych i kategorie osób

1. Rodzaje danych osobowych oraz kategorie osób, których dane dotyczą, zostały określone w Załączniku nr 1.

2. Administrator oświadcza, że jest uprawniony do powierzenia przetwarzania danych osobowych wskazanych w Załączniku nr 1 oraz że dane te są przetwarzane zgodnie z RODO.
3. Administrator ponosi odpowiedzialność za zgodność z prawem wprowadzania danych do systemu oraz za ich prawidłowość i aktualność.

§ 5. Obowiązki Administratora

1. Administrator oświadcza, że posiada podstawę prawną do przetwarzania danych osobowych powierzanych Procesorowi, w tym w szczególności podstawę uprawniającą do powierzenia ich przetwarzania.
2. Administrator jest obowiązany do:
3. zapewnienia spełnienia obowiązków informacyjnych wobec osób, których dane dotyczą;
4. realizacji praw osób, których dane dotyczą, przy pomocy Procesora na zasadach określonych w § 8;
5. aktualizacji zakresu powierzenia w przypadku zmiany celów lub rodzajów przetwarzanych danych;
6. poinformowania Procesora o szczególnych kategoriach danych osobowych, jeżeli są one przetwarzane w systemie.
7. Administrator zobowiązuje się do nieprzetwarzania w systemie danych osobowych w zakresie szerszym niż określony w Załączniku nr 1, chyba że zakres ten został rozszerzony na piśmie.

§ 6. Obowiązki Procesora

1. Procesor przetwarza dane osobowe wyłącznie w zakresie i celach określonych w niniejszej Umowie oraz na udokumentowane polecenie Administratora.
2. Procesor zobowiązuje się do:
3. zapewnienia, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub podlegały odpowiedniemu ustawowemu obowiązkowi poufności;
4. przetwarzania danych osobowych wyłącznie na podstawie udokumentowanych poleceń Administratora;
5. zapewnienia, aby dane osobowe nie były udostępniane podmiotom trzecim bez zgody Administratora, z zastrzeżeniem § 11;
6. informowania Administratora o każdym przypadku, gdy przetwarzanie miałoby odbywać się z naruszeniem RODO lub poleceń Administratora;
7. prowadzenia rejestru kategorii czynności przetwarzania w rozumieniu art. 30 ust. 2 RODO.
8. Procesor nie wykorzystuje danych osobowych do celów innych niż wynikające z Umowy głównej, w tym nie wykorzystuje ich do własnych celów marketingowych.

§ 7. Poufność

1. Osoby, które w imieniu Procesora wykonują czynności związane z przetwarzaniem danych osobowych, są zobowiązane do zachowania poufności.
2. Procesor zapewnia, że dostęp do danych osobowych mają wyłącznie osoby upoważnione, w zakresie niezbędnym do realizacji Umowy głównej.

§ 8. Bezpieczeństwo przetwarzania

1. Procesor, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw osób fizycznych, wdraża odpowiednie środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku, w tym w szczególności:
2. szyfrowanie danych osobowych w trakcie transmisji (TLS);
3. zapewnienie ciągłej poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
4. regularne testowanie, ocenianie i ocenę skuteczności środków technicznych i organizacyjnych;
5. kontrolę dostępu opartą o zasadę minimalnych uprawnień;
6. tworzenie kopii zapasowych danych w zakresie określonym w Umowie głównej.
7. Procesor zapewnia, aby środki bezpieczeństwa były adekwatne do charakteru przetwarzanych danych.

§ 9. Pomoc Administratorowi w realizacji praw osób

1. Procesor, w zakresie swoich możliwości technicznych, pomaga Administratorowi w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania praw wynikających z RODO, w tym prawa dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych oraz sprzeciwu.
2. Procesor bezzwłocznie informuje Administratora o otrzymanych żądaniach osób, których dane dotyczą, i nie odpowiada na nie samodzielnie, chyba że Administrator wyrazi na to zgodę lub wynika to z przepisów prawa.
3. Procesor udostępnia Administratorowi narzędzia umożliwiające realizację praw osób, jeżeli są one dostępne w ramach systemu.

§ 10. Pomoc przy naruszeniach ochrony danych

1. Procesor bezzwłocznie, nie później niż w ciągu 4 godzin od powzięcia wiadomości, informuje Administratora o stwierdzonym Naruszeniu ochrony danych.
2. Zgłoszenie, o którym mowa w ust. 1, zawiera w szczególności:

- opis charakteru naruszenia, w tym kategorie i przybliżoną liczbę osób oraz rekordów, których dotyczy;
- imię i nazwisko oraz dane kontaktowe osoby kontaktowej;
- opis prawdopodobnych konsekwencji naruszenia;
- opis zastosowanych i planowanych środków zaradczych.

1. Procesor pomaga Administratorowi w wypełnieniu obowiązku zgłoszenia naruszenia właściwemu organowi nadzorczemu oraz zawiadomienia osób, których dane dotyczą, jeżeli obowiązek taki ciąży na Administratorze.
2. Procesor prowadzi dokumentację wszystkich naruszeń, w tym okoliczności, skutki oraz podjęte działania naprawcze.

§ 11. Audyty i kontrole

1. Administrator ma prawo, po uprzednim zawiadomieniu z wyprzedzeniem 5 dni roboczych, do przeprowadzenia audytu lub kontroli zgodności przetwarzania z niniejszą Umową oraz RODO.
2. Audyt nie może zakłócać bieżącego funkcjonowania usługi ani naruszać poufności danych innych klientów Procesora.
3. Administrator może żądać od Procesora informacji niezbędnych do wykazania zgodności z obowiązkami wynikającymi z art. 28 RODO.
4. Koszty nadmiernie częstych lub rozszerzonych audytów obciążają Administratora.

§ 12. Podwykonawcy / Subprocesorzy

1. Administrator wyraża ogólną zgodę na korzystanie przez Procesora z Subprocesorów.
2. Procesor informuje Administratora o każdej planowanej zmianie dotyczącej dodania lub zastąpienia Subprocesorów, z wyprzedzeniem 5 dni, dając Administratorowi możliwość zgłoszenia sprzeciwu.
3. W przypadku zgłoszenia sprzeciwu przez Administratora wobec nowego Subprocesora, Administrator może rozwiązać Umowę główną ze skutkiem na koniec bieżącego okresu rozliczeniowego, jeżeli Procesor nie wskaże alternatywnego rozwiązania.
4. Procesor nakłada na Subprocesorów obowiązki w zakresie ochrony danych odpowiadające obowiązkom wynikającym z niniejszej Umowy, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych.
5. Procesor ponosi odpowiedzialność wobec Administratora za działania i zaniechania Subprocesorów.
6. Aktualna lista Subprocesorów stanowi Załącznik nr 2 do niniejszej Umowy.

§ 13. Hosting i infrastruktura

1. Usługa SaaS jest świadczona z wykorzystaniem infrastruktury hostingowej dostawcy usług chmurowych (OVHcloud lub inny dostawca wskazany przez Procesora), który działa jako Subprocesor w rozumieniu § 12.
2. Lokalizacja przetwarzania danych: Europejski Obszar Gospodarczy (EOG)

3. Procesor zapewnia, że Subprocesor świadczący usługi hostingowe przetwarza dane osobowe wyłącznie na udokumentowane polecenie Procesora i Administratora oraz zobowiązany jest do zachowania poufności.

§ 14. Transfer danych poza EOG

1. W przypadku, gdy przetwarzanie danych osobowych wiąże się z transferem danych poza Europejski Obszar Gospodarczy, Strony zobowiązują się do zapewnienia odpowiednich zabezpieczeń w rozumieniu art. 44–49 RODO, w tym w szczególności standardowych klauzul umownych zatwierdzonych decyzją Komisji Europejskiej.
2. Procesor informuje Administratora o zamiarze transferu danych poza EOG przed jego rozpoczęciem, wskazując państwo docelowe oraz podstawę transferu.
3. Jeżeli transfer poza EOG nie został uzgodniony, Procesor nie dokonuje transferu danych poza EOG bez uprzedniej zgody Administratora.

§ 15. Dokumentowanie zgodności

1. Procesor prowadzi dokumentację niezbędną do wykazania zgodności z obowiązkami wynikającymi z art. 28 RODO, w tym rejestr czynności przetwarzania.
2. Procesor udostępnia Administratorowi na żądanie informacje niezbędne do wykazania zgodności z RODO.

§ 16. Postępowanie w przypadku incydentu bezpieczeństwa

1. Procesor wdraża procedury postępowania w przypadku incydentu bezpieczeństwa, w tym procedury wykrywania, zgłaszania i usuwania skutków incydentów.
2. Procesor bezzwłocznie informuje Administratora o incydentach mających wpływ na bezpieczeństwo danych osobowych, zgodnie z § 10.
3. Procesor podejmuje niezwłoczne działania naprawcze mające na celu ograniczenie skutków incydentu oraz zapobieżenie jego powtórzeniu.

§ 17. Usunięcie lub zwrot danych po zakończeniu usługi

1. Po zakończeniu świadczenia usługi Procesor, na polecenie Administratora, usuwa lub zwraca Administratorowi wszystkie dane osobowe oraz usuwa istniejące kopie, chyba że przepisy prawa wymagają ich przechowywania.
2. Procesor zapewnia usunięcie danych osobowych z infrastruktury hostingowej po upływie okresu przechowywania, nie później niż w terminie 30 dni od zakończenia usługi.
3. Na żądanie Administratora Procesor potwierdza na piśmie usunięcie danych osobowych.

§ 18. Odpowiedzialność

1. Procesor ponosi odpowiedzialność za szkody wyrządzone przetwarzaniem, jeżeli nie dopełnił obowiązków określonych w RODO skierowanych do podmiotów przetwarzających lub działał poza zgodnym z prawem poleceniem Administratora lub wbrew temu poleceniu.
2. Odpowiedzialność Stron jest ograniczona na zasadach określonych w Umowie głównej.

§ 19. Postanowienia końcowe

1. Niniejsza Umowa stanowi załącznik do Umowy głównej i obowiązuje przez okres jej obowiązywania.
2. W sprawach nieuregulowanych niniejszą Umową zastosowanie mają przepisy RODO oraz prawa polskiego.
3. Zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Wszelkie spory rozstrzyga sąd właściwy dla siedziby Procesora.

Załącznik nr 1 — Opis przetwarzania danych

Cel przetwarzania	Rodzaj danych	Kategorie osób	Operacje przetwarzania	Okres przechowywania
Świadczenie usługi SaaS — udostępnianie systemu	Dane identyfikacyjne, kontaktowe, dane kont użytkowników oraz inne dane wprowadzane przez Klienta do systemu	Pracownicy, współpracownicy, klienci, kontrahenci i inne osoby, których dane Klient wprowadza do systemu	Gromadzenie, przechowywanie, porządkowanie, przeglądanie, modyfikowanie, udostępnianie techniczne, usuwanie	Przez okres obowiązywania Umowy głównej oraz do 30 dni od zakończenia usługi
Administrowanie środowiskiem	Dane kont użytkowników, dane techniczne, adresy IP, logi systemowe i informacje diagnostyczne, jeśli są rejestrowane	Użytkownicy systemu i osoby korzystające z usługi	Dostęp techniczny, konfiguracja, monitorowanie, diagnostyka i zabezpieczanie środowiska	Przez okres niezbędny do zapewnienia bezpieczeństwa i prawidłowego działania usługi, zgodnie z przyjętą retencją
Wsparcie techniczne	Dane zgłoszeń, dane kontaktowe zgłaszających oraz dane z systemu niezbędne do diagnozy problemu	Użytkownicy systemu i osoby wskazane w zgłoszeniach	Przeglądanie, analiza, diagnostyka, a w uzasadnionych przypadkach modyfikowanie danych	Przez okres niezbędny do obsługi zgłoszenia i udokumentowania jego rozwiązania, zgodnie z przyjętą retencją
Tworzenie kopii zapasowych	Dane przechowywane w systemie, w tym dane osobowe zawarte w bazie danych i plikach	Kategorie osób odpowiadające danym objętym kopią zapasową	Kopiowanie, przechowywanie, odtwarzanie w przypadku awarii i usuwanie	Zgodnie z cyklem retencji kopii zapasowych, nie dłużej niż przez określony w umowie okres retencji backupów

Załącznik nr 2 — Lista Subprocesorów

Lp.	Nazwa Subprocesora	Rodzaj usługi	Lokalizacja przetwarzania
1.	OVHcloud	Hosting infrastruktury serwerowej, uruchamianie systemu i przechowywanie danych	Europejski Obszar Gospodarczy (EOG)
2.	Microsoft Corporation / Microsoft Ireland Operations Limited — zgodnie z właściwymi warunkami usługi Azure	Przechowywanie plików i kopii danych w Azure Blob Storage	Europejski Obszar Gospodarczy (EOG)