UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH (DPA) dla usług SaaS PHU ELKA Radosław Miczyński

1. Wprowadzenie.

Niniejsza umowa stanowi Załącznik nr 2 do Regulaminu świadczenia usług SaaS i zostaje zawarta na podstawie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).

2. Strony i role

Administratorem danych osobowych jest Klient korzystający z usług SaaS świadczonych przez PHU ELKA Radosław Miczyński.

Podmiotem przetwarzającym (Procesorem) jest:

PHU ELKA Radosław Miczyński,
ul. Kosowa 3A, 66-008 Wilkanowo,
NIP: 929-101-93-67, REGON: 970083265.

Strony zawierają niniejszą Umowę powierzenia w związku z zawarciem umowy o świadczenie usług SaaS.

3. Przedmiot i czas trwania powierzenia

Administrator powierza Procesorowi przetwarzanie danych osobowych w zakresie niezbędnym do realizacji usług SaaS.

Powierzenie przetwarzania danych obowiązuje przez czas trwania umowy SaaS oraz przez okres czynności końcowych po jej zakończeniu.

Umowa ma charakter akcesoryjny wobec Regulaminu Świadczenia Usług SaaS.

4. Zakres i cel przetwarzania

Dane osobowe przetwarzane są wyłącznie w celu:

- świadczenia usług SaaS,
- utrzymania i rozwoju systemów,
- zapewnienia bezpieczeństwa i ciągłości działania.

Zakres przetwarzania obejmuje w szczególności:

- utrwalanie, przechowywanie, modyfikowanie,
- udostępnianie w ramach Systemu SaaS,
- usuwanie lub przekazywanie kopii danych po zakończeniu umowy.

Rozwój funkcjonalności systemu odbywa się bez wykorzystywania danych osobowych powierzonych przez Administratora, chyba że Administrator wyraźnie dopuści takie wykorzystanie w odrębnej podstawie prawnej.

Procesor przetwarza dane wyłącznie w celu realizacji Umowy oraz zgodnie z udokumentowanymi poleceniami Administratora i nie jest uprawniony do samodzielnego określania celów przetwarzania.

5. Kategorie danych i osób

Kategorie danych osobowych:

- dane identyfikacyjne,
- dane kontaktowe,
- dane zawodowe i organizacyjne,
- dane techniczne i eksploatacyjne (np. adres IP, logi),
- inne dane wprowadzone przez Administratora do Systemu SaaS.

Kategorie osób, których dane dotyczą

- pracownicy i współpracownicy Administratora,
- klienci i kontrahenci,
- użytkownicy systemów SaaS.

6. Obowiązki Procesora i instrukcje Administratora

Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, w tym w zakresie przekazywania danych do państwa trzeciego lub organizacji międzynarodowej, chyba że obowiązek taki wynika z przepisów prawa.

Za udokumentowane polecenia Administratora uznaje się w szczególności:
- postanowienia niniejszej Umowy oraz Umowy głównej,
- konfigurację usług dokonaną przez Administratora w ramach systemu,
- polecenia przekazywane za pośrednictwem systemu obsługi zgłoszeń, poczty elektronicznej lub innych uzgodnionych kanałów komunikacji,
- inne udokumentowane instrukcje przekazane przez Administratora.

Procesor niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane polecenie narusza RODO lub inne przepisy o ochronie danych osobowych.

W przypadku, o którym mowa w ust. 3, Procesor ma prawo wstrzymać wykonanie polecenia do czasu jego wyjaśnienia lub zmiany przez Administratora.

Procesor prowadzi rejestr kategorii czynności przetwarzania wykonywanych w imieniu Administratora, jeżeli jest do tego zobowiązany na podstawie przepisów prawa.

Procesor wdraża i utrzymuje środki techniczne i organizacyjne zgodne z art. 32 RODO oraz wdrożonym Systemem Zarządzania Bezpieczeństwem Informacji ISO 27001.

7. Audyty i wykazanie zgodności

Procesor udostępnia Administratorowi – na uzasadnione żądanie – wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz niniejszej Umowie, w tym w szczególności informacje dotyczące stosowanych środków technicznych i organizacyjnych, polityk bezpieczeństwa oraz wykorzystywanych podmiotów przetwarzających.

Procesor umożliwia Administratorowi lub upoważnionemu przez niego audytorowi przeprowadzenie audytu lub inspekcji w zakresie zgodności przetwarzania danych z niniejszą Umową oraz RODO, na następujących zasadach:
- audyt odbywa się po uprzednim powiadomieniu z co najmniej 14-dniowym wyprzedzeniem,
- audyt jest przeprowadzany w godzinach pracy Procesora i w sposób niezakłócający jego działalności,
- zakres audytu jest ograniczony do informacji niezbędnych do weryfikacji zgodności,
- Administrator zapewnia, że audytor jest związany obowiązkiem poufności.

Procesor może zaproponować przeprowadzenie audytu w formie zdalnej lub udostępnienie aktualnych raportów z audytów (np. ISO, testy bezpieczeństwa) jako alternatywy dla audytu na miejscu, o ile zapewniają one równoważny poziom weryfikacji.

Wykonywanie uprawnień audytowych odbywa się z poszanowaniem tajemnicy przedsiębiorstwa Procesora, bezpieczeństwa systemów oraz praw innych klientów.

Jeżeli audyt wykaże istotne naruszenia niniejszej Umowy lub przepisów prawa, Procesor niezwłocznie podejmie działania naprawcze i poinformuje Administratora o ich wdrożeniu.

8. Środki techniczne i organizacyjne

Procesor stosuje środki techniczne i organizacyjne zapewniające:
- poufność,
- integralność,
- dostępność danych.

Szczegółowy opis zabezpieczeń zawarty jest w dokumencie: *Środki techniczne i organizacyjne stosowane w PHU ELKA*.

Procesor zapewnia ciągłe doskonalenie zabezpieczeń zgodnie z analizą ryzyka.

9. Podpowierzenie danych

Administrator wyraża ogólną zgodę na korzystanie przez Procesora z podmiotów przetwarzających (subprocesorów) w celu realizacji Umowy.

Lista podmiotów podprzetwarzających udostępniana jest Administratorowi na żądanie.

Procesor informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia subprocesorów, z co najmniej 14-dniowym wyprzedzeniem.

Administrator ma prawo zgłosić uzasadniony sprzeciw wobec takiej zmiany w terminie 14 dni od dnia otrzymania informacji.

W przypadku zgłoszenia sprzeciwu Strony podejmą negocjacje w dobrej wierze w celu rozwiązania sytuacji, w szczególności poprzez zmianę sposobu świadczenia usług.

W przypadku braku możliwości uzgodnienia rozwiązania, Administrator ma prawo wypowiedzieć Umowę główną w zakresie usług objętych zmianą subprocesora ze skutkiem natychmiastowym.

Procesor zapewnia, że każdy subprocesor podlega obowiązkom ochrony danych co najmniej równoważnym z niniejszą Umową.

10. Przekazywanie danych poza UE/EOG

Dane osobowe przetwarzane przez Procesora nie są przekazywane poza Europejski Obszar Gospodarczy (EOG).

Jeżeli w związku z realizacją Umowy dochodzi do przekazania danych poza EOG, Procesor zapewnia, że transfer odbywa się wyłącznie na podstawie odpowiednich zabezpieczeń przewidzianych w RODO, w szczególności: a) decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony, lub b) standardowych klauzul umownych (SCC) przyjętych przez Komisję Europejską.

Aktualna lista podmiotów przetwarzających oraz dostawców, którym dane mogą być przekazywane poza EOG, wraz ze wskazaniem podstawy transferu, jest dostępna pod stałym adresem internetowym wskazanym przez Procesora lub w załączniku do niniejszej Umowy.

Procesor informuje Administratora o planowanych zmianach w zakresie transferów poza EOG zgodnie z zasadami określonymi w §8 (Podpowierzenie).

Na uzasadnione żądanie Administratora Procesor udostępnia informacje dotyczące zastosowanych zabezpieczeń transferu, w zakresie niezbędnym do wykazania zgodności z RODO.

11. Naruszenia ochrony danych

Procesor zgłasza Administratorowi naruszenie ochrony danych osobowych bez zbędnej zwłoki, nie później niż w ciągu 48 godzin od momentu potwierdzenia naruszenia.

Zgłoszenie naruszenia przekazywane jest za pośrednictwem uzgodnionego kanału komunikacji (np. e-mail, system zgłoszeniowy) i obejmuje co najmniej:

- opis charakteru naruszenia,
- kategorie i przybliżoną liczbę osób, których dane dotyczą,
- kategorie i przybliżoną liczbę rekordów danych,
- możliwe konsekwencje naruszenia,
- środki zastosowane lub proponowane w celu zaradzenia naruszeniu oraz ograniczenia jego skutków,
- dane kontaktowe osoby lub zespołu odpowiedzialnego za obsługę incydentu.

Jeżeli przekazanie wszystkich informacji nie jest możliwe w tym samym czasie, Procesor przekazuje je sukcesywnie, bez zbędnej zwłoki.

Procesor współpracuje z Administratorem w zakresie analizy naruszenia, oceny ryzyka oraz realizacji obowiązków zgłoszeniowych wobec organu nadzorczego i osób, których dane dotyczą.

12. Pomoc Administratorowi

Procesor wspiera Administratora w realizacji:

- praw osób, których dane dotyczą,
- obowiązków wynikających z art. 32–36 RODO w zakresie technicznie i organizacyjnie możliwym.

13. Zakończenie przetwarzania danych

Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych, w zależności od decyzji Administratora, Procesor:

- zwraca Administratorowi dane osobowe w ustrukturyzowanym, powszechnie używanym formacie elektronicznym (np. CSV), lub
- usuwa dane osobowe.

Zwrot lub usunięcie danych następuje nie później niż w terminie 90 dni od zakończenia Umowy głównej, chyba że obowiązujące przepisy prawa wymagają ich dalszego przechowywania.

Procesor usuwa dane ze wszystkich systemów produkcyjnych oraz środowisk pomocniczych, z zastrzeżeniem ust. 4.

Dane mogą być przechowywane w kopiach zapasowych przez okres wynikający z polityki retencji Procesora, jednak w tym czasie nie będą aktywnie przetwarzane i zostaną trwale usunięte zgodnie z cyklem nadpisywania kopii zapasowych.

Logi systemowe zawierające dane osobowe są przechowywane przez ograniczony okres wynikający z polityki bezpieczeństwa i retencji logów, a następnie usuwane lub anonimizowane.

Na żądanie Administratora Procesor potwierdza usunięcie danych osobowych.

Do momentu usunięcia lub zwrotu danych Procesor zapewnia ich ochronę zgodnie z niniejszą Umową.

Dane usuwane są zgodnie z polityką retencji i procedurami SZBI.

14. Odpowiedzialność

Odpowiedzialność Procesora wobec Administratora może podlegać ograniczeniom określonym w Umowie głównej (Regulaminie SaaS), w zakresie dopuszczalnym przez obowiązujące przepisy prawa.

Żadne postanowienie niniejszej Umowy ani Umowy głównej nie wyłącza ani nie ogranicza odpowiedzialności Procesora w zakresie, w jakim taka odpowiedzialność nie może zostać wyłączona lub ograniczona na mocy RODO lub innych przepisów powszechnie obowiązującego prawa.

W szczególności ograniczenia odpowiedzialności nie mają zastosowania w przypadku naruszenia obowiązków wynikających z bezwzględnie obowiązujących przepisów prawa, w tym RODO.

15. Postanowienia końcowe

Niniejsza umowa posiada oznaczenie wersji oraz datę obowiązywania.
W sprawach nieuregulowanych zastosowanie mają:

- Regulamin Świadczenia Usług SaaS,
- przepisy RODO,
- prawo polskie.

Załącznik wchodzi w życie z dniem zawarcia Umowy SaaS i stanowi jej integralną część.