Umowa powierzenia przetwarzania danych osobowych

zawarta w Kobylnicy, dnia _____ pomiędzy:

(zwana dalej „Umową")

_____

_____

_____

*(*dane podmiotu, który umowę zawiera)*

zwany w dalszej części umowy **„Administratorem Danych"**
reprezentowanym przez:

_____

oraz

AB-Com Arkadiusz Bednarczyk, ul.Wodna 19A, 76-251 Kobylnica
wpisaną w dniu 2007-08-08 do rejestru ewidencji działalności gospodarczej prowadzonej przez Wójta Gminy Kobylnica pod numerem 1978, identyfikującym się numerem NIP 8391244413, REGON:771558618

zwany w dalszej części umowy **„Procesorem"**,
reprezentowanym przez:
Arkadiusza Bednarczyka

zwanymi dalej łącznie „Stronami"

§ 1

Przedmiot i czas trwania umowy

1. Administrator Danych powierza Procesorowi, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Procesor zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Procesor oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.
4. Umowa zostaje zawarta na czas obowiązywania Umowy Głównej – po jej wygaśnięciu niniejsza umowa staje się nieważna.
5. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem 30-dniowego okresu wypowiedzenia.
6. W przypadku wygaśnięcia umowy głównej lub wypowiedzenia niniejszej umowy Procesor zobowiązuje się do usunięcia powierzonych danych w nieprzekraczalnym terminie 30 dni.

§2

Zakres i cel przetwarzania danych

1. Przedmiot, charakter i cel ewentualnego gromadzenia, przetwarzania lub wykorzystywania danych osobowych, rodzaju danych i osób, których dotyczą, zostały uzupełnione przez Administratora Danych i przedstawione Procesorowi zgodnie z **Załącznikiem 1** niniejszego dokumentu.

§3

Obowiązki i prawa Procesora

1. Procesor zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia. Szczegółowy wykaz zabezpieczeń oraz zakres ich zastosowania określony został w **Załączniku 2** niniejszej umowy.
2. Procesor zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Procesor zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.

4. Procesor zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich jak i po jego ustaniu.
5. Procesor po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Procesor pomaga Administratorowi Danych w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Procesor po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi Danych w ciągu 24 godzin.
8. Procesor nie jest uprawniony do wstrzymywania lub ograniczania przetwarzania danych osobowych przez Administratora Danych. W przypadku otrzymania przez Procesora zgłoszenia naruszeń praw do przetwarzania od osoby, której dane są przetwarzane zostanie ono niezwłocznie przekazane Administratorowi Danych.
9. Procesor ma prawo żądać potwierdzenia w formie tekstowej poleceń od Administratora Danych.
10. Procesor powinien niezwłocznie poinformować Administratora Danych, jeśli w jego ocenie polecenie narusza przepisy o ochronie danych. Procesor ma wówczas prawo zawiesić wykonanie odpowiednich instrukcji, dopóki Administrator Danych nie potwierdzi lub nie zmieni tych instrukcji.

11. Procesor ma prawo domagać się zwrotu kosztów obsługi osób zgłaszających naruszenia praw do przetwarzania danych osobowych przez Administratora Danych, jak również wynagrodzenia za wykonywanie poleceń zleconych przez Administratora Danych. Wysokość wynagrodzenia zostanie ustalona na podstawie stałej stawki godzinowej pracownika Procesora.

§4

Prawo kontroli

1. Administrator Danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Procesora przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator Danych realizować będzie prawo kontroli w godzinach pracy Procesora i z minimum 14-dniowym jego uprzedzeniem.
3. Procesor zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora Danych, nie dłuższym niż 14 dni.
4. Procesor udostępnia Administratorowi Danych wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
5. Procesor może domagać się zwrotu kosztów pracy pracownika wyznaczonego do asysty prac audytora. Wysokość wynagrodzenia zostanie ustalona na podstawie stałej stawki godzinowej pracownika Procesora.

§5

Dalsze powierzenie danych do przetwarzania

1. Procesor może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora Danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora Danych, chyba że obowiązek taki nakłada na Procesora prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Procesor. W takim przypadku przed rozpoczęciem przetwarzania Procesor informuje Administratora Danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §5 ust. 1 Umowy, winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Procesora w niniejszej Umowie.
4. Procesor ponosi pełną odpowiedzialność wobec Administratora Danych za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Procesora

1. Procesor jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Procesor zobowiązuje się do niezwłocznego poinformowania Administratora Danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Procesora danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Procesora, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Procesora tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora Danych.

§7

Rozwiązanie umowy

1. Administrator Danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Procesor:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora Danych.

§8

Zasady zachowania poufności

1. Procesor zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora Danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Procesor oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora Danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

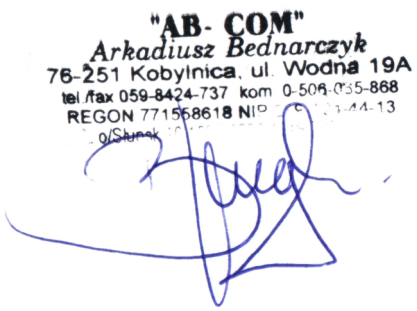
§9

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. Prawem właściwym dla niniejszej umowy będzie prawo polskie.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu Cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Procesora.

Administrator Danych

Procesor



Załącznik 1 do umowy powierzenia przetwarzania danych osobowych

Wykaz danych osobowych oraz cel ich przetwarzania

Rodzaj danych

Przedmiotem umowy są następujące rodzaje i kategorie danych osobowych:

Cel przetwarzania danych

Powierzone przez Administratora Danych dane osobowe będą przetwarzane przez Procesora wyłącznie w celu:

Osoby dotknięte przetwarzaniem

Wykaz osób, których umowa obejmuje:

Administrator Danych

Załącznik 2 do umowy powierzenia przetwarzania danych osobowych

Środki techniczne i organizacyjne zastosowane zgodnie z art. 32 GDPR i poprawkami

1. Poufność

Zabezpieczenie dostępu fizycznego
Parki centrów danych znajdują się w Nürnberg i Falkenstein w Niemczech, prowadzone są przez firmę Hetzner Online GmbH i posiadają następujące zabezpieczenia dostępu fizycznego:

- elektroniczny system kontroli wejścia fizycznego z dziennikiem
- ogrodzenia obwodowe o wysokim poziomie bezpieczeństwa wokół całego parku centrów danych
- udokumentowana dystrybucja kluczy dla pracowników i klientów kolokacji do szaf kolokacyjnych (każdy klient ma dostęp tylko do swojej szafy)
- personel centrum danych jest obecny 24 godziny na dobę, 7 dni w tygodniu
- system blokowania drzwi bezpieczeństwa
- wejście do budynku serwerowni jest dozwolone tylko w obecności pracownika firmy Hetzner Online
- monitoring i nadzór wideo dla wszystkich wejść i wyjść

Elektroniczna kontrola dostępu

Serwery dedykowane i VPS

- hasła dostępu do usług są generowane automatycznie podczas procesu instalacji systemu i przekazywane bezpośrednio Administratorowi Danych drogą mailową lub wyświetlane w panelu administracyjnym
- zmiana haseł dostępowych może być przeprowadzona tylko przez Administratora Danych i nie są one znane Procesorowi

Konta hostingowe, pocztowe oraz serwery zarządzane

- hasła dostępu do usług są generowane podczas procesu rejestracji kont i przesyłane jednorazowo drogą mailową lub wyświetlane w panelu administracyjnym
- zmiana haseł może być przeprowadzona przez Administratora Danych lub na życzenie generowana i przesyłana w panelu administracyjnym przez Procesora, który nie ma wglądu do wygenerowanego hasła

Wewnętrzna kontrola dostępu

- Procesor dokonuje zabezpieczeń wewnętrznych systemów informatycznych przed nieuprawnionym dostępem poprzez regularne aktualizacje bezpieczeństwa przy użyciu najnowocześniejszych znanych mu technologii
- Procesor stosuje politykę bezpieczeństwa w przyznawaniu dostępu do swoich systemów informatycznych dla upoważnionych i przeszkolonych pracowników
- dla serwerów dedykowanych i VPS zabezpieczenie przed nieuprawnionym dostępem leży po stronie Administratora Danych

- dla kont hostingowych i serwerów zarządzanych zabezpieczeniem systemów informatycznych przed nieuprawnionym dostępem zajmuje się Procesor. Do obowiązków Administratora Danych należy zabezpieczyć dostęp do posiadanych haseł oraz loginów.

Zabezpieczenie nośników danych

- dyski znajdujące się w serwerach, które zostały wycofane z użycia są wielokrotnie czyszczone zgodnie z polityką ochrony danych wypowiedzianych umów. Po dokładnych testach napędy są przeznaczone do ponownego wykorzystania.
- uszkodzone dyski, które nie mogą być poddane bezpiecznemu czyszczeniu są fizycznie niszczone w centrum danych w Falkenstein.

Kontrola izolacji danych i pseudonimizacji

- wewnętrzne systemy Procesora posiadają fizyczną lub logiczną izolację od pozostałych danych. Kopie tych danych są również tworzone przy użyciu podobnych systemów fizycznej lub logicznej izolacji.
- w przypadku serwerów dedykowanych i VPS za izolację danych odpowiada Administrator Danych.
- w przypadku kont hostingowych i serwerów zarządzanych fizyczna i logiczna izolacja danych i kopii jest zapewniona przez Procesora.
- odpowiedzialność za pseudonimizację leży po stronie Administratora Danych.

2. Integralność

Kontrola przepływu danych

- wszyscy pracownicy Procesora są przeszkoleni zgodnie z art. 32 ust. 4 GDPR i są zobowiązani do zapewnienia, że dane osobowe są przetwarzane zgodnie z przepisami o ochronie danych.
- po rozwiązaniu umowy następuje usunięcie danych zgodnie z przepisami o ochronie danych.
- Procesor zapewnia szyfrowaną transmisję danych dla oferowanych usług.

Kontrola wprowadzanych danych

- w wewnętrznych systemach informatycznych Procesora dane są wprowadzane lub gromadzone przez Administratora Danych. Zmiany w danych są logowane.
- w przypadku serwerów dedykowanych i VPS odpowiedzialność za kontrolę wprowadzanych danych ponosi Administrator Danych.
- w przypadku kont hostingowych i serwerów zarządzanych dane są wprowadzane lub gromadzone przez Administratora Danych. Zmiany w danych są logowane.

3. Dostępność i odporność systemów

Kontrola dostępności

Wewnętrzne systemy administracyjne Procesora

- polityka tworzenia i przywracania kopii bezpieczeństwa, z zastosowaniem dziennych kopii wszystkich istotnych danych
- profesjonalne zastosowanie programów zabezpieczających (skanerów antywirusowych, zapór ogniowych, programów szyfrujących, filtrów antyspamowych)
- stosowanie technologii RAID na wszystkich kluczowych serwerach
- monitoring wszystkich kluczowych serwerów
- zastosowanie systemu zasilania bezprzerwowego lub awaryjnego systemu zasilania
- trwale aktywna ochrona DDoS

Serwery dedykowane i VPS

- wykonywanie kopii bezpieczeństwa leży po stronie Administratora Danych
- zastosowanie systemu zasilania bezprzerwowego lub awaryjnego systemu zasilania
- trwale aktywna ochrona DDoS

Konta hostingowe i serwery zarządzane

- polityka tworzenia i przywracania kopii bezpieczeństwa, z wykonywaniem kopii baz danych 3 razy w tygodniu oraz raz w tygodniu pełnej kopii plików – przechowywane na odseparowanych serwerach backupowych w dodatkowych dwóch kopiach tygdniowych
- udostępnione oprogramowanie do ręcznego i automatycznego tworzenia własnych kopii bezpieczeństwa
- stosowanie technologii RAID
- zastosowanie systemu zasilania bezprzerwowego lub awaryjnego systemu zasilania
- trwale aktywna ochrona DDoS

Szybkie działania naprawcze

- We wszystkich systemach wewnętrznych istnieje zdefiniowany łańcuch eskalacji, który określa, kto ma być informowany w przypadku błędu, aby przywrócić system tak szybko, jak to możliwe.

4. Procedury regularnego testowania, mierzenia i oceniania skuteczności

- przy tworzeniu oprogramowania domyślnie brane są pod uwagę ustawienia dotyczące ochrony danych osobowych
- oprogramowanie jest stale testowane pod kątem ochrony danych osobowych
- wdrożone zarządzanie reagowaniem na incydenty
- kontrola zgód i umów zgodnie z wytycznymi dotyczącymi przetwarzania danych.