Umowa powierzenia przetwarzania danych osobowych (DPA)

Wersja obowiązująca od dnia 02-09-2026 r.

sporządzona na podstawie art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO)

§1. Postanowienia ogólne

1. Niniejsza umowa powierzenia przetwarzania danych osobowych (dalej: **„DPA"**) zostaje zawarta pomiędzy:
   - **Klientem** — osobą fizyczną, prawną lub jednostką organizacyjną, która zawarła z Usługodawcą umowę o świadczenie Usług (dalej: **„Administrator"** w rozumieniu RODO) — o ile Klient przetwarza dane osobowe osób trzecich w ramach Usługi,
   - a **CYBERMONKEY SP. Z O.O.** z siedzibą w Warszawie, al. Jana Pawła II 43A/37B, 01-001 Warszawa, KRS 0000911855 (dalej: **„Procesor"** w rozumieniu RODO, w Regulaminie określany jako Usługodawca).
2. DPA stanowi załącznik nr 3 do Regulaminu świadczenia usług. Akceptacja Regulaminu przez Klienta obejmuje zawarcie DPA w zakresie niezbędnym do świadczenia Usługi.
3. DPA znajduje zastosowanie wyłącznie w przypadku, gdy Klient przetwarza w ramach Usługi dane osobowe osób trzecich jako administrator w rozumieniu art. 4 pkt 7 RODO. DPA nie znajduje zastosowania, gdy Klient korzysta z Usługi w ramach czynności o czysto osobistym lub domowym charakterze (art. 2 ust. 2 lit. c RODO), w szczególności prowadząc prywatny serwer gry dostępny wyłącznie dla ograniczonego kręgu znajomych; w takim przypadku Klient nie występuje jako administrator danych Graczy, a przetwarzanie danych Klienta przez Usługodawcę regulują Regulamin i Polityka Prywatności.
4. Administrator pozostaje administratorem danych osobowych w rozumieniu art. 4 pkt 7 RODO w odniesieniu do danych osobowych graczy i innych osób trzecich przetwarzanych w ramach Usługi (dalej: **„Dane"**). Procesor przetwarza Dane wyłącznie w imieniu Administratora i na jego polecenie.

§2. Przedmiot i zakres powierzenia

1. Administrator powierza Procesorowi przetwarzanie Danych osób trzecich, w szczególności:
   - adresy IP graczy łączących się z serwerem,
   - identyfikatory graczy (np. UUID, nick),
   - logi połączeń i aktywności graczy na serwerze,
   - inne dane osobowe przekazywane przez graczy do systemu serwera gry.
2. Przetwarzanie obejmuje w szczególności następujące czynności: przechowywanie, organizowanie, modyfikowanie, pobieranie, korzystanie, udostępnianie na polecenie Administratora, ograniczanie, usuwanie — wyłącznie w zakresie i w celu niezbędnym do świadczenia Usługi.

3. Przetwarzanie dotyczy następujących kategorii osób, których dane dotyczą: gracze łączący się z serwerem Administratora, użytkownicy korzystający z funkcji serwera.
4. Przetwarzanie dotyczy następujących kategorii danych: dane identyfikacyjne (nick, UUID), dane techniczne (adres IP, dane urządzenia), logi aktywności.
5. Czas trwania powierzenia: przez okres trwania umowy o świadczenie Usług oraz przez 30 dni po jej zakończeniu (grace period) w celu umożliwienia Administratorowi pobrania danych.

§3. Obowiązki Procesora

1. Procesor przetwarza Dane **wyłącznie na udokumentowane polecenie Administratora**, w tym w odniesieniu do transferu danych do państwa trzeciego lub organizacji międzynarodowej, o ile nie jest to wymagane przez prawo Unii Europejskiej lub prawa państwa członkowskiego, do którego Procesor podlega; w takim przypadku Procesor informuje Administratora o tym wymogie prawnym przed przetwarzaniem, chyba że prawo zabrania takiego informowania ze względu na ważny interes publiczny.
2. Procesor zapewnia, że osoby upoważnione do przetwarzania Danych zobowiązały się do zachowania poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania poufności.
3. Procesor podejmuje wszelkie wymagane środki techniczne i organizacyjne określone w §5, w celu zabezpieczenia Danych.
4. Procesor nie powierza przetwarzania Danych innemu podmiotowi (subprocesorowi) bez uprzedniej, wyraźnej lub ogólnej autoryzacji Administratora. W przypadku ogólnej autoryzacji Procesor informuje Administratora o każdej planowanej zmianie dotyczącej dodania lub zastąpienia subprocesora, dając Administratorowi możliwość wyrażenia sprzeciwu wobec takiej zmiany.
5. Procesor, uwzględniając charakter przetwarzania, w możliwie największym stopniu wspiera Administratora poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z jego obowiązku odpowiadania na żądania osób, których dane dotyczą, dotyczące wykonywania ich praw na podstawie rozdziału III RODO.
6. Procesor wspiera Administratora w zapewnieniu zgodności z obowiązkami określonymi w art. 32–36 RODO, z uwzględnieniem rodzaju przetwarzania oraz informacji dostępnych dla Procesora.
7. Procesor udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności z art. 28 RODO oraz umożliwia i wspiera audyty, w tym inspekcje, przeprowadzane przez Administratora lub podmiot przez niego upoważniony, z zastrzeżeniem §6.
8. Procesor niezwłocznie informuje Administratora w przypadku stwierdzenia, że polecenie Administratora narusza RODO lub inne przepisy o ochronie danych.

§4. Subprocesorzy

1. Administrator wyraża ogólną autoryzację na powierzenie przetwarzania Danych przez Procesora następującym kategoriom subprocesorów: dostawcom infrastruktury centrów danych, dostawcom usług IT niezbędnych do świadczenia Usługi, dostawcom usług ochrony i bezpieczeństwa (w tym anty-DDoS).

2. Aktualny wykaz subprocesorów jest dostępny w Serwisie lub na żądanie pod adresem rodo@mchost.pl. Procesor informuje Administratora o zmianie subprocesorów z co najmniej 14-dniowym wyprzedzeniem na adres e-mail podany przez Administratora.

3. W przypadku braku sprzeciwu Administratora w terminie 14 dni od powiadomienia, zmiana subprocesora uważana jest za zaakceptowaną. W przypadku sprzeciwu Procesor może: a) zaproponować innego subprocesora, b) rozwiązać DPA z zachowaniem terminu wypowiedzenia wynikającego z umowy o świadczenie Usług.

4. Procesor zawiera z każdym subprocesorem umowę powierzenia zapewniającą poziom ochrony danych nie niższy niż wynikający z niniejszej DPA.

§5. Środki bezpieczeństwa

1. Procesor stosuje następujące środki techniczne i organizacyjne w celu zabezpieczenia Danych:

Środki techniczne:
a) szyfrowanie transmisji danych (TLS 1.2+),
b) szyfrowanie dysków (at-rest encryption),
c) firewall i systemy IDS/IPS,
d) ochrona anty-DDoS,
e) regularne aktualizacje bezpieczeństwa systemów operacyjnych i aplikacji,
f) kontrola dostępu oparta na rolach (RBAC),
g) dwuskładnikowe uwierzytelnianie (2FA) dla dostępu administracyjnego,
h) automatyczne monitorowanie i alertowanie o anomaliach,
i) regularne testy bezpieczeństwa (co najmniej raz na 12 miesięcy).

Środki organizacyjne:
a) zasada minimalizacji dostępu (need-to-know),
b) obowiązek zachowania poufności dla wszystkich osób upoważnionych,
c) procedura zarządzania incydentami bezpieczeństwa,
d) procedura zarządzania cyklem życia dostępu (onboarding/offboarding),
e) rejestr kategorii czynności przetwarzania (art. 30 RODO).

1. Procesor ocenia i w razie potrzeby aktualizuje środki bezpieczeństwa, dostosowując je do stanu techniki, kosztów wdrożenia, charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych.

§6. Prawo audytu

1. Administrator ma prawo przeprowadzenia audytu zgodności przetwarzania Danych przez Procesora z niniejszą DPA oraz z RODO.

2. Audyt może być przeprowadzony **nie częściej niż raz na 12 miesięcy**, z co najmniej **30-dniowym wyprzedzeniem** pisemnym (w tym elektronicznym), po uzgodnieniu terminu z Procesorem.

3. **[B2B]** Koszty audytu ponosi Administrator. Audyt nie może zakłócać normalnego funkcjonowania infrastruktury Procesora ani wpływać na dostępność Usług dla innych Klientów.

4. Przed przystąpieniem do audytu Administrator lub podmiot przez niego upoważniony zobowiązuje się do podpisania umowy o poufności (NDA).
5. W przypadku podmiotu upoważnionego przez Administratora do przeprowadzenia audytu, podmiot taki musi być niezależnym audytorem posiadającym odpowiednie kwalifikacje i niebędącym bezpośrednim konkurentem Procesora.
6. Procesor udostępnia na żądanie Administratora certyfikaty zgodności i raporty z niezależnych audytów bezpieczeństwa (np. SOC 2 Type II, ISO 27001) w zastępstwie audytu własnego Administratora, jeżeli takie certyfikaty posiada.

§7. Naruszenie ochrony danych

1. Procesor niezwłocznie — nie później niż w terminie **48 godzin** od stwierdzenia naruszenia — informuje Administratora o każdym naruszeniu ochrony Danych, które może stanowić naruszenie praw lub wolności osób, których dane dotyczą.
2. Zgłoszenie zawiera w szczególności:
   a) opis naruszenia, w tym kategorię i przybliżoną liczbę osób, których dane dotyczą, oraz kategorii i przybliżonej ilości Danych,
   b) nazwę i dane kontaktowe osoby kontaktowej udzielającej dodatkowych informacji,
   c) opis prawdopodobnych skutków naruszenia,
   d) opis środków podjętych lub proponowanych przez Procesora w celu zaradzenia naruszeniu, w tym — w stosownych przypadkach — środków ograniczających możliwe negatywne skutki.
3. Procesor dokumentuje wszelkie naruszenia ochrony Danych, w tym okoliczności naruszenia, jego skutki oraz podjęte środki zaradcze, i udostępnia tę dokumentację Administratorowi na żądanie.

§8. Usuwanie i zwrot danych

1. Po zakończeniu świadczenia Usług Procesor, na polecenie Administratora, **zwraca Dane Administratorowi** w standardowym formacie (np. SQL dump, JSON, CSV) lub **usuwa je**, chyba że prawo Unii Europejskiej lub prawa państwa członkowskiego wymaga przechowania Danych.
2. Zwrot lub usunięcie następuje w terminie **30 dni** od dnia zakończenia umowy o świadczenie Usług (grace period), chyba że Administrator zażąda wcześniejszego zwrotu.
3. Po upływie grace period Dane, które nie zostały pobrane przez Administratora, podlegają trwałemu usunięciu z infrastruktury Procesora w terminie kolejnych 14 dni.
4. Procesor potwierdza Administratorowi usunięcie Danych na żądanie.

§9. Postanowienia końcowe

1. DPA podlega prawu polskiemu.
2. W sprawach nieuregulowanych DPA stosuje się przepisy RODO oraz Regulamin świadczenia usług.
3. DPA wchodzi w życie z chwilą zawarcia umowy o świadczenie Usług.
4. DPA wygasa z chwilą upływu grace period określonego w §8.

5. Jeżeli którekolwiek postanowienie DPA okaże się nieważne lub bezskuteczne, pozostałe postanowienia pozostają w mocy.

MCHOST

CYBERMONKEY Sp. z o.o
Al. Jana Pawła II 43A/37B
01-001 Warszawa

NIP	REGON	KRS
7441827778	389514743	0000911855

Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego.
Kapitał Zakładowy 5.000,00 PLN w całości opłacony.