AM Holding Group — Aneks o przetwarzaniu danych (publiczny, bez podpisów)

Wersja: 1.0 · Wejście w życie: z chwilą zamówienia lub pierwszego użycia usług AMHG
Strony: niniejszy DPA ma zastosowanie, gdy AM Holding Group (AMHG, Podmiot przetwarzający) przetwarza dane osobowe w imieniu Klienta (Administrator) na podstawie umowy/zamówienia/warunków (Umowa).
Prawo: RODO (Rozporządzenie (UE) 2016/679) oraz prawo polskie.
Język: Obowiązuje wersja polska; tłumaczenia UA/ENG są pomocnicze.
Akceptacja: Złożenie zamówienia, użycie formularzy na stronie lub skorzystanie z usług oznacza akceptację DPA.

1. **Definicje**
   Pojęcia z art. 4 RODO: dane osobowe, przetwarzanie, osoba, administrator, procesor podmiot przetwarzający, naruszenie ochrony danych, organ nadzorczy, państwo trzecie. „SCC" — standardowe klauzule umowne UE 2021/914.

2. **Zakres i role**
   AMHG przetwarza dane wyłącznie w celu świadczenia usług z Umowy i Aneksu I, wyłącznie na udokumentowane polecenia Klienta Administratora (art. 28 ust. 3 lit. a RODO).

3. **Poufność i personel**
   AMHG zapewnia poufność i szkolenia osób upoważnionych dopuszczonych do przetwarzania danych.

4. **Bezpieczeństwo**
   AMHG stosuje środki techniczne i organizacyjne (Aneks II) adekwatne do ryzyka (art. 32 RODO), w tym kontrolę dostępu, szyfrowanie, kopie zapasowe, monitoring, zarządzanie incydentami i zmianami.

5. **Podprzetwarzający**
   Klient Administrator upoważnia AMHG do korzystania z podprzetwarzających z listy w Aneksie III (publicznej i aktualnej). AMHG nakłada równoważne obowiązki ochrony danych i informuje o istotnych zmianach, umożliwiając uzasadniony sprzeciw.

6. **Transfery międzynarodowe**
   Domyślnie lokalizacje w UE/EOG. Przetwarzanie/dostęp w państwie trzecim wyłącznie z zabezpieczeniami wg Aneksu IV (SCC 2021/914 Moduły 2/3, UK IDTA/Addendum, TIA oraz środki z Aneksu II).

7. **Wsparcie Administratora**
   AMHG zapewnia rozsądną pomoc w realizacji praw osób, obowiązkach bezpieczeństwa/DPIA/konsultacji oraz dostarcza informacje niezbędne do wykazania zgodności.

8. **Zgłoszenie naruszenia**
   AMHG powiadamia Klienta Administratora bez zbędnej zwłoki po stwierdzeniu naruszenia; wewnętrzny cel: do 48 godzin od potwierdzenia; współpraca i działania naprawcze.

9. **Rejestry i audyty**
   AMHG prowadzi rejestry z art. 30(2). Po 14 dniach uprzedzenia, nie częściej niż raz na 12 miesięcy, Klient Administrator może przeprowadzić audyt lub przejrzeć niezależne raporty; audyt nie może zakłócać pracy, musi chronić poufność/bezpieczeństwo; koszty ponoszą strony.

10. **Zwrot i usunięcie**
    Po zakończeniu usług lub na polecenie Klienta Administratora AMHG zwraca lub usuwa dane (wraz z kopiami) w rozsądnym czasie, o ile prawo nie wymaga retencji. Domyślne okresy logów — w Aneksie I.

11. **Odpowiedzialność i pierwszeństwo**
    Odpowiedzialność stron wynika z Umowy. W razie kolizji w zakresie ochrony danych, pierwszeństwo ma niniejszy DPA.

12. **Zmiany**
    AMHG może aktualizować Aneksy III–IV i inne postanowienia; o istotnych zmianach informuje z wyprzedzeniem, jeśli to możliwe.

Kontakt ds. prywatności: go@amhg.eu • Adres: Katowice, Polska (UE)

Aneks I — Szczegóły przetwarzania
Usługi (cel): zarządzane usługi IT — wirtualizacja (KVM-VM), storage, sieci i bezpieczny zdalny dostęp, monitoring/observability, telefonia IP, hosting/VDS, migracje (w tym UA→UE), wsparcie.
Kategorie osób: pracownicy/kontraktorzy Administratora Klienta, użytkownicy/klienci, dostawcy/kontakty.
Rodzaje danych: imię i nazwisko, stanowisko, służbowe dane kontaktowe, dane uwierzytelniania i autoryzacji, identyfikatory techniczne (IP, user-agent), logi systemowe/bezpieczeństwa, metadane konfiguracji; metadane połączeń i nagrania tylko gdy funkcja jest włączona przez Administratora Klienta.
Szczególne kategorie: nie planowane; wymagają pisemnej instrukcji i dodatkowych zabezpieczeń.
Operacje: zbieranie, przechowywanie, dostęp, przekazywanie transmisja, monitoring, backup/restore, usuwanie.
Retencja (domyślnie): logi 90–365 dni; backupy/nagrania — wg polityki Administratora Klienta.
Lokalizacje: UE/EOG; państwa trzecie wyłącznie na warunkach Aneksu IV.
Odbiorcy: upoważniony personel AMHG; podprzetwarzający (Aneks III).

Aneks II — Środki techniczne i organizacyjne bezpieczeństwa
Dostęp i tożsamość: indywidualne konta, minimalne uprawnienia, dostęp oparty na rolach, uwierzytelnianie wieloskładnikowe dla kont administracyjnych, kontrola sesji, logowanie dostępu.
Sieć i systemy: segmentacja, zapory sieciowe, bezpieczna zdalna administracja (VPN), utwardzanie konfiguracji, terminowe aktualizacje, zarządzanie podatnościami.
Ochrona danych: szyfrowanie w tranzycie (TLS) i w spoczynku (gdzie dostępne), ograniczony dostęp do kluczy, weryfikacja integralności.
Kopie zapasowe i odtworzenie: regularne backupy; migawki w punktach w czasie i replikacja tam, gdzie włączone; testy odtworzeniowe.
Monitoring i logowanie: monitoring 24/7, scentralizowane logi, alerty z eskalacją; ścieżki audytu odporne na manipulacje.
Reagowanie na incydenty: procedury, szybkie działania naprawcze, analizy po incydencie.
Zarządzanie zmianą i dostawcami: akceptacje i plany wycofania; due diligence dostawców; DPA/SCC z podprzetwarzającymi.
Bezpieczeństwo fizyczne: centra danych w UE/EOG z kontrolą dostępu, monitoringiem wizyjnym, redundancją zasilania/chłodzenia.
Personel i poufność: wdrożenie/szkolenia, NDA, zasada „need-to-know".
Ciągłość działania: plany DR/BCP zgodnie z wymaganym poziomem usług.

Aneks III — Podprzetwarzający
Publiczna, aktualna lista pod /legal/subprocessors (nazwa, funkcja, kraj, podstawa prawna). Typowe kategorie: DC i łączność w UE/EOG; narzędzia monitoringu/serwis-desk/dokumentacji; operatorzy telekom (jeśli używana telefonia); lokalizacje backup/DR w UE. Powiadomienia o zmianach i prawo do uzasadnionego sprzeciwu.

Aneks IV — Transfery międzynarodowe
SCC 2021/914 (Moduły 2/3) + TIA + środki z Aneksu II. UK: IDTA lub UK Addendum. Migracje UA→UE: domyślne przetwarzanie w UE/EOG; dalsze transfery tylko z równoważnymi zabezpieczeniami.