AM Holding Group — Додаток щодо обробки персональних даних (публічна версія)

Версія: 1.0 • Набрання чинності: з моменту замовлення або першого користування послугами AMHG
Сторони: цей Додаток (DPA) застосовується, коли AM Holding Group (AMHG, Процесор) обробляє персональні дані від імені Клієнта (Контролер) за будь-яким договором/замовленням/умовами (Договір).
Право: GDPR (Регламент (ЄС) 2016/679) та право Польщі.
Мова: Чинною є польська версія; український та английский тексти надані для зручності.
Акцепт: Надсилання замовлення, використання форм на сайті чи отримання послуг означає погодження з цим DPA.

1. **Визначення**
   Терміни GDPR: персональні дані, обробка, суб'єкт даних, контролер, процесор, порушення захисту даних, наглядовий орган, третя країна. «SCC» — стандартні договірні положення ЄС 2021/914.

2. **Обсяг і ролі**
   AMHG обробляє дані виключно для надання послуг, визначених у Договорі та Додатку I, лише за документованими інструкціями Клієнта (ст. 28(3)(a) GDPR).

3. **Конфіденційність і персонал**
   AMHG забезпечує конфіденційність та навчання уповноважених осіб, які мають доступ до даних.

4. **Безпека**
   AMHG впроваджує технічні та організаційні заходи (Додаток II) відповідно до ризиків (ст. 32 GDPR), зокрема контроль доступу, шифрування, резервування, моніторинг, управління інцидентами та змінами.

5. **Субпроцесори**
   Клієнт уповноважує AMHG залучати субпроцесорів зі списку в Додатку III (публічний, актуальний). AMHG накладає рівноцінні обов'язки щодо захисту даних і повідомляє про суттєві зміни з правом обґрунтованого заперечення.

6. **Міжнародні передання**
   Локації за замовчуванням — ЄС/ЄЕЗ. Будь-який доступ/обробка у третій країні — лише з гарантіями за Додатком IV (SCC 2021/914 Модулі 2/3, за потреби UK IDTA/Addendum, TIA та заходи безпеки з Додатку II).

7. **Допомога Контролеру**
   AMHG надає розумну допомогу з виконанням запитів суб'єктів, вимог безпеки/DPIA/попередніх консультацій і надає інформацію для демонстрації відповідності.

8. **Повідомлення про інцидент**
   AMHG повідомляє Клієнта без зволікань після підтвердження інциденту; цільовий внутрішній строк — до 48 годин; AMHG взаємодіє з Клієнтом щодо повідомлень і виправних дій.

9. **Облік та аудит**
   AMHG веде записи за ст. 30(2). За 14 днів попередження, не частіше ніж раз на 12 міс., Клієнт може провести аудит або переглянути незалежні звіти; аудит не має порушувати конфіденційність/безпеку чи роботу; витрати — за кожною стороною.

10. **Повернення та видалення**
    Після припинення послуг або за письмовою інструкцією AMHG повертає або видаляє дані (включно з копіями) у розумні строки, якщо закон не зобов'язує зберігати. Типові строки для журналів — у Додатку I.

11. **Відповідальність і пріоритет**
    Відповідальність сторін визначено Договором. У питаннях захисту даних пріоритет має цей DPA.

12. **Зміни**
    AMHG може оновлювати Додатки III–IV та інші положення; про суттєві зміни повідомляється заздалегідь, якщо це можливо.

Контакт з приватності: go@amhg.eu • Адреса: Катовіце, Польща (ЄС)

Додаток I — Деталі обробки
Послуги (мета): керовані IT-послуги — віртуалізація (KVM-віртуальні машини), сховище, мережі та безпечний віддалений доступ, моніторинг/спостережність, IP-телефонія, хостинг/VDS, міграції (вкл. UA→EU), підтримка.
Категорії суб'єктів: працівники/підрядники Клієнта, користувачі/клієнти, постачальники/контакти.
Типи даних: ім'я, посада, службові контакти, дані автентифікації та авторизації, технічні ідентифікатори (IP, user-agent), журнали систем/безпеки, метадані конфігурацій; метадані дзвінків і записи — лише якщо функцію увімкнено Клієнтом.
Спеціальні категорії: не передбачені; у разі потреби — лише за письмовою інструкцією та з додатковими гарантіями.
Операції: збирання, зберігання, доступ, передавання, моніторинг, резервне копіювання/відновлення, видалення.
Зберігання (типово): журнали 90–365 днів; бекапи/записи — за політикою Клієнта.
Локації: ЄС/ЄЕЗ; треті країни — лише на умовах Додатку IV.
Одержувачі: уповноважений персонал AMHG; субпроцесори (Додаток III).

Додаток II — Технічні та організаційні заходи безпеки
Доступ і ідентифікація: індивідуальні облікові записи, принцип мінімально необхідних прав, доступ за ролями, багатофакторна автентифікація для адміністраторів, контроль сесій, журнали доступу.
Мережа та системи: сегментація, мережеві екрани, безпечне віддалене адміністрування (VPN), посилення конфігурацій, своєчасні оновлення, керування вразливостями.
Захист даних: шифрування під час передавання (TLS) та під час зберігання (де підтримується), обмежений доступ до ключів, перевірка цілісності.
Резервне копіювання та відновлення: регулярні резервні копії; знімки «у точці часу» та реплікація за потреби; документовані тести відновлення.
Моніторинг і журнали: моніторинг 24/7, централізовані журнали, сповіщення з ескалацією; аудит-трейл із ознаками втручання.
Реагування на інциденти: затверджені інструкції, оперативне реагування, аналіз та усунення причин.
Керування змінами та постачальниками: погодження змін і плани відкату; оцінка постачальників; DPA/SCC із субпроцесорами.
Фізична безпека: дата-центри в ЄС/ЄЕЗ із контролем доступу, відеонаглядом, резервуванням живлення/охолодження.
Персонал і конфіденційність: онбординг/підвищення обізнаності, NDA, принцип «потрібно знати».
Безперервність: плани аварійного відновлення/безперервності, якщо це вимагається рівнем послуги.

Додаток III — Субпроцесори
Публічний поточний список на /legal/subprocessors (назва, функція, країна, правова підстава). Типові категорії: ЦОД і провайдери мережі в ЄС/ЄЕЗ; інструменти моніторингу/сервіс-деску/документації; телеком-оператори (якщо використовується телефонія); майданчики резервного копіювання/DR у ЄС. Повідомлення про зміни з правом обґрунтованого заперечення.

Додаток IV — Міжнародні передавання
SCC 2021/914 (Модулі 2/3) + оцінка впливу передання (TIA) + заходи з Додатку II. Для UK — IDTA або UK Addendum. Для міграцій UA→EU — розміщення/обробка за замовчуванням у ЄС/ЄЕЗ; подальші передавання — лише з еквівалентними гарантіями.