AM Holding Group — Data Processing Addendum (Public, no signatures)

Version: 1.0 • Effective date: upon ordering or first use of AMHG services
Parties: This Data Processing Addendum ("DPA") applies where AM Holding Group ("AMHG", Processor) processes Personal Data on behalf of the Client ("Controller") under any master agreement, order, or terms (the "Agreement").
Governing law: EU General Data Protection Regulation (EU 2016/679, "GDPR") and Polish law.
Language: Polish version controls. English and Polish versions are provided for convenience.
Acceptance: By placing an order, using forms on the site, or receiving services, Controller accepts this DPA.

1. **Definitions**
   "Personal Data", "Processing", "Data Subject", "Controller", "Processor", "Personal Data Breach", "Supervisory Authority", "Third Country" have the meanings in GDPR Art. 4. "SCC" means the EU Standard Contractual Clauses 2021/914.

2. **Scope and roles**
   AMHG processes Personal Data solely to provide services described in the Agreement and Annex I, only on documented instructions from Controller (GDPR Art. 28(3)(a)).

3. **Confidentiality and personnel**
   AMHG ensures authorised persons are bound by confidentiality and receive appropriate training.

4. **Security**
   AMHG implements technical and organisational measures (Annex II) appropriate to risk (GDPR Art. 32), including access control, encryption, backups, monitoring, incident and change management.

5. **Sub-processing**
   Controller authorises AMHG to use sub-processors listed in Annex III (public, always-current list). AMHG imposes equivalent data-protection obligations and will notify of material changes with a right to raise reasonable, justified objections.umożliwiający zarządzanie Usługami, dostępami, płatnościami, zgłoszeniami technicznymi oraz danymi Klienta.

6. **International transfers**
   Default locations are in the EU/EEA. Any third-country access/processing occurs only with safeguards per Annex IV (SCC 2021/914 Modules 2/3, UK IDTA/Addendum where applicable, TIA, and the measures in Annex II).

7. **Assistance to Controller**
   AMHG will reasonably assist with Data Subject requests, security/DPIA/prior consultation duties, and provide information necessary to demonstrate compliance.

8. **Personal Data Breach notification**
   AMHG will notify Controller without undue delay after becoming aware of a Personal Data Breach; target internal window: within 48 hours of confirmation; AMHG will cooperate and remediate.

9. **Records and audits**
   AMHG maintains Art. 30(2) records. Upon 14 days' notice, not more than once per 12 months, Controller may audit or review independent reports; audits must protect confidentiality/security and avoid disruption; each party bears own costs.

10. **Return and deletion**
    Upon termination or written instruction, AMHG will delete or return Personal Data (and delete copies) within commercially reasonable time unless law requires retention. Default operational log retention: see Annex I.

11. **Liability and precedence**
    Liability follows the Agreement. For data-protection conflicts, this DPA prevails.

12. **Changes**
    AMHG may update Annex III (sub-processors) and Annex IV (transfer tools); material changes will be notified in advance where feasible. Other DPA updates apply upon publication unless Controller objects on reasonable grounds.

Privacy contact: go@amhg.eu · Address: Katowice, Poland (EU)

Annex I — Details of Processing
Services (purpose): managed infrastructure services: virtualization (KVM-based VMs), storage, networks and secure remote access, monitoring/observability, IP telephony, hosting/VDS, migration (including UA→EU), support.
Data Subjects: Controller staff/contractors; Controller users/customers; suppliers/contacts.
Data types: name, role, business email/phone, authentication/authorisation data, technical identifiers (IP, user-agent), system/security logs, configuration metadata; call metadata and recordings only if the feature is enabled by Controller.
Special categories: not intended; any such processing requires written instruction and extra safeguards.
Operations: collection, storage, access, transmission, monitoring, backup/restore, deletion.
Retention (defaults): operational/security logs 90–365 days; backups/recordings per Controller policy.
Locations: EU/EEA by default; any third-country access only under Annex IV safeguards.
Recipients: AMHG authorised staff; approved sub-processors (Annex III).

Annex II — Technical and Organisational Measures
Access & identity: unique accounts, least privilege, role-based access, multi-factor authentication for admin access, session controls, access logging.
Network & systems: segmentation, firewalls, secure remote administration (VPN), configuration hardening, timely patching, vulnerability management.
Data protection: TLS in transit; encryption at rest where supported; restricted key access; integrity checks.
Backups & recovery: scheduled backups; point-in-time snapshots and replication where enabled; documented restore tests.
Monitoring & logging: 24/7 monitoring, centralised logs, alerting with escalation; tamper-evident audit trails.
Incident response: defined runbooks, prompt breach handling, post-incident reviews.
Change/vendor management: approvals and rollback plans; supplier due diligence; DPAs/SCCs.
Physical security: EU/EEA data centres with access control, CCTV, power/cooling redundancy.
Staff & confidentiality: onboarding/awareness; NDAs; need-to-know.
Continuity: documented DR/BCP where required by service level.

Annex III — Authorised Sub-processors
Public, living list at /legal/subprocessors (name, function, country, legal basis). Typical categories: EU/EEA data centre & network providers; monitoring/service desk/documentation tools; telephony carriers (if used); EU backup/DR sites.
Notice of changes with right to raise justified objections.

Annex IV — International Transfers
Safeguards: EU SCC 2021/914 (Modules 2/3) + TIA + Annex II measures. UK: IDTA or UK Addendum. UA→EU migrations: default hosting/processing in EU/EEA; onward transfers only with equivalent safeguards.