HATI Privacy Addendum - GCC and Middle East

High-level regional privacy supplement for UAE, KSA, Qatar, and related financial-free-zone considerations.

Regional legal review strongly recommended. Privacy and data-transfer rules in the GCC can vary materially between federal regimes, sector regulators, and financial free zones. Use this addendum as a starter only and finalize it with local counsel for the markets where HATI is actually offered.

1. Scope

This Addendum supplements the HATI Global Privacy Notice for deployments or users in the Gulf Cooperation Council and nearby Middle East markets, including use cases involving the United Arab Emirates, the Kingdom of Saudi Arabia, and the State of Qatar.

HATI is software developed and managed by Blokketen Solutions Inc. It is intended to sit above a customer's existing banks and approved payment providers and may involve cross-border access to data, support teams, and infrastructure.

2. Regional framework note

Depending on the circumstances, applicable privacy obligations may arise under UAE federal privacy law, the Saudi Personal Data Protection Law, Qatar's Personal Data Privacy Protection Law, or other local regimes.

If a relevant entity operates in a financial free zone, separate data-protection frameworks may also apply, including the ADGM Data Protection Regulations 2021 and the DIFC Data Protection Law No. 5 of 2020.

3. Transparency, purpose limitation, and role allocation

Blokketen Solutions Inc. should clearly identify whether it acts as an independent controller for website, security, billing, and relationship-management functions, or whether it acts only on the documented instructions of a customer for operational workflow data.

Customers should ensure that they have an appropriate legal basis to upload payroll, vendor, onboarding, or payment-workflow data into HATI, particularly where that data includes identifiers, national IDs, bank details, or other information treated as sensitive or regulated under local law.

4. Cross-border transfers and localization

Cross-border data access or transfer may require additional notices, contractual protections, impact assessments, regulator filings, or localization controls depending on the applicable jurisdiction and the categories of data involved.

Before launch, confirm the final hosting architecture, support model, subprocessor list, and transfer mechanism for each country where HATI will be used.

5. Data-subject requests and regulator engagement

Individuals may have rights under applicable law to request information about processing, obtain access, request correction, request deletion where appropriate, object or withdraw consent in some situations, or file a complaint with a competent regulator.

Requests should first be directed to the privacy contact in the Global Privacy Notice. If Blokketen Solutions Inc. processes the relevant data only on behalf of a customer, the request may need to be handled by that customer.

6. Operational drafting checklist before publication

- confirm the correct contracting entity and its place of establishment;
- confirm whether any customer data stays in-country or must be accessible only through controlled remote support channels;
- confirm whether a free-zone regime such as ADGM or DIFC applies to any part of the deployment;
- confirm whether customer onboarding, KYB, sanctions, or regulated-provider relationships create additional recordkeeping or notice obligations; and
- insert regulator, complaint, and contact language that matches the final jurisdiction.