Tilda: Your Partner in Secure Learning and Change Design

Executive Summary

Tilda (Hey Tilda AB) is committed to ensuring the confidentiality, integrity, and availability of customer data. Our platform is designed with privacy and security as core principles. We maintain an Information Security Management System (ISMS) managed by Vanta aligned with ISO/IEC 27001:2022, and work towards full ISO 27001 certification. Our security program covers data protection, incident response, business continuity, and compliance with the EU General Data Protection Regulation (GDPR).

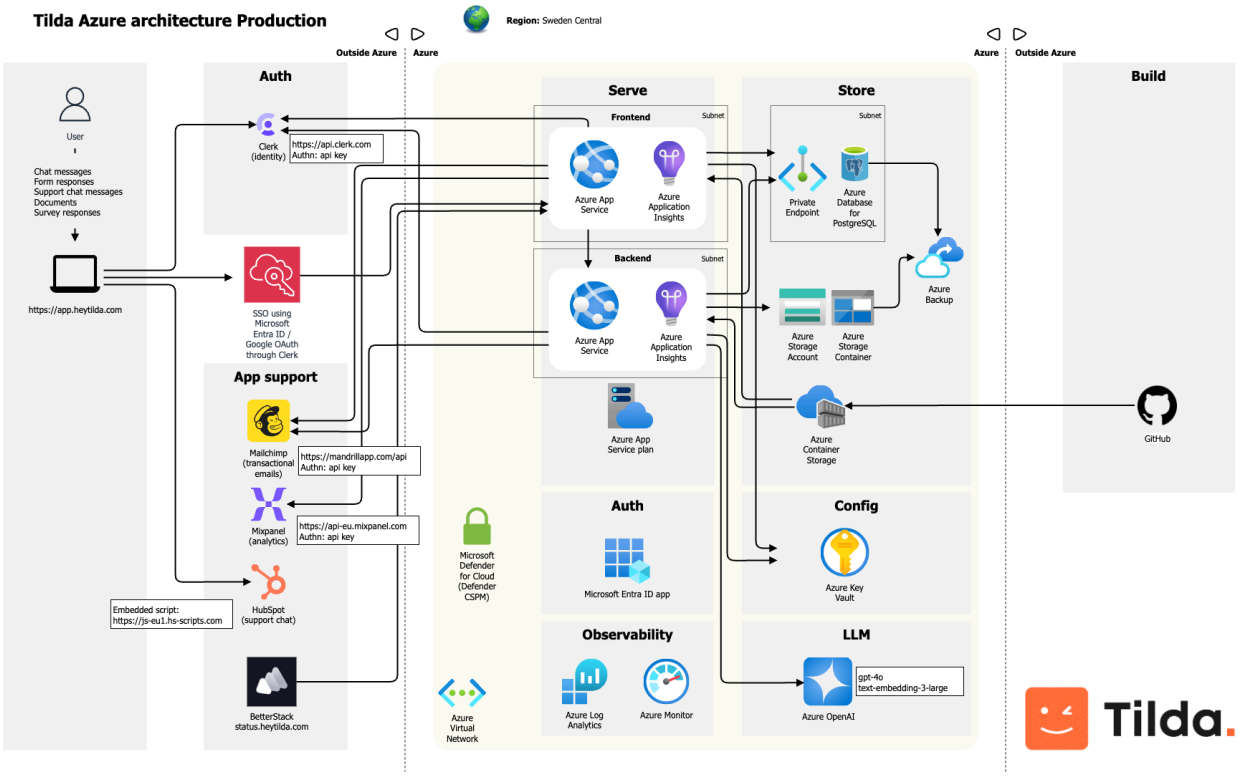
Security at a Glance

Area	Status
Hosting	Secure cloud infrastructure on Microsoft Azure
LLM Provider	Microsoft Azure OpenAI
Data encryption	AES-256 at rest, TLS 1.2/1.3 in transit
Identity & Access (Infrastructure)	MFA enforced, RBAC, least privilege, Microsoft Entra PIM (Privileged Identity Management) where applicable
Identity & Access (Clients)	SSO using OAuth2 Social Sign On (Microsoft, Google)
Incident Response	72 h breach notification
Business Continuity	RTO ≤ 24h / RPO ≤ 24h
Compliance	GDPR aligned, working towards ISO 27001 certification. ISMS managed by Vanta.
Sub-processors	Reviewed annually, under DPA and Data Privacy Framework

Platform & Infrastructure Security

Tilda is built on secure cloud infrastructure with a shared responsibility model. We apply network segmentation, firewalls, and intrusion detection. Data is encrypted at rest and in transit, access is controlled through MFA and role-based access control (RBAC). Secure development practices, including code reviews, static and dynamic analysis (SAST/DAST), and dependency scanning, are enforced throughout our software development lifecycle.

Solution Architecture



Data Protection & Privacy

We maintain a GDPR-aligned privacy program integrated into our ISMS. Our program includes:

- Data inventory and flow mapping
- Data subject rights handling (DSAR, erasure, portability)
- Breach notification procedures (≤72 hours)
- Sub-processor due diligence and safeguards (DPAs, SCCs, DPF)
- Privacy by design and default throughout our SDLC.

Compliance & Certifications

Our Information Security Management System (ISMS) is operational and designed to meet ISO 27001:2022 requirements, working towards full certification. We are GDPR compliant and conduct regular internal audits and risk reviews.

Business Continuity & Disaster Recovery

Our Business Continuity and Disaster Recovery Plan addresses scenarios such as network outages, malware/ransomware, theft, and natural disasters. Critical systems and roles are defined, communication strategies outlined, and dependencies on cloud providers documented. Our Recovery Time Objective (RTO) is ≤24 hours and our Recovery Point Objective (RPO) is ≤24 hours. Encrypted backups are performed.

Incident Response

We maintain a formal Incident Response Plan (IRP) including severity levels, escalation paths, and breach notification requirements. Customers are notified without undue delay and within 72 hours if their data is impacted. Post-incident reviews ensure continuous improvement.

Employee Security & Training

All employees complete mandatory security and GDPR training during onboarding and annually thereafter. Training covers phishing, secure development, incident reporting, and acceptable use.

Shared Responsibility Model

We clearly define what Tilda secures (infrastructure, platform, encryption, incident response) and what customers are responsible for (managing user access and data entered into the platform).

Appendix

- Trust Center with a full list of ISMS & privacy policies available upon request.
- Current list of sub-processors published at https://www.heytilda.com/security
- For security inquiries, contact security@heytilda.com