Data Protection & Compliance Overview

This document provides an in-depth look at Tekle Holographics' approach to data protection, privacy, and regulatory compliance. It is intended for data protection officers, compliance teams, and legal stakeholders within our client organizations who want to understand how Tekle meets its obligations under laws like GDPR, how we handle personal and sensitive data, and how we ensure compliance with specific industry regulations (such as ITAR for defense). We cover our policies, technical measures, and contractual commitments in detail, giving you a clear picture of our data stewardship.

GDPR and Global Privacy Compliance

Tekle Holographics operates in alignment with the European Union's **General Data Protection Regulation (GDPR)** and equivalent data protection laws worldwide. We treat privacy as a fundamental right and integrate GDPR principles into our business processes and product design.

Lawfulness, Fairness, and Transparency: Tekle only processes personal data if there is a legitimate basis to do so (usually because it is necessary to provide our services as per our contract with the customer, or with individual consent for specific features). We are transparent about our data practices: our Privacy Notice (available on our website) clearly describes what personal data we collect, how we use it, who we share it with (if anyone), and how long we keep it. We ensure that individuals using Tekle's services (for example, operators of our holographic systems or participants in collaborative sessions) have access to this information and can exercise control where applicable (such as opting out of non-essential data collection).

Data Minimization and Purpose Limitation: As a policy, Tekle minimizes personal data collection. Our holographic visualization products typically process large amounts of **enterprise data** (e.g., BIM models, geospatial data, engineering designs), which generally do not involve personal information. The personal data we do handle is limited to user account information (name, business email, login credentials) and usage logs. We do not collect sensitive personal data like home addresses, social security numbers, or biometrics of end users – except in rare cases where a client might use our system to display such data as part of their content (in which case it remains their data and we process it only within that context, e.g., if a client visualized a personnel database holographically, those personal records stay within their control). Tekle will never use personal data we process for our own independent purposes such as marketing or profiling, unless expressly authorized by the individual (for instance, if someone signs up for our newsletter separately from using the product).

Data Subject Rights: Under GDPR, individuals have rights such as access to their data, rectification of inaccuracies, erasure (the "right to be forgotten"), restriction of processing, data portability, and objection to processing. When Tekle is the Data Processor for our customer (the Data Controller), we assist our customer in fulfilling these rights. Practically, if one of our customer's employees asks to have their account data removed from Tekle systems, the customer can either self-service delete the user via our admin interface or send us a request and we will ensure all personal data related to that user is erased (except any data we must keep for legal reasons, which we will communicate). We have processes in place to handle such requests promptly – internal KPIs ensure we handle access or deletion requests well within the one-month GDPR timeframe (usually we do it in under a week, often a day or two). For data portability requests, since we usually process data that originates from our customer's systems, the portable format is often the original files or models. However, for any personal data we store, we can export it in a structured, commonly used format (e.g., CSV or JSON for account info, log excerpts in CSV).

Data Security (Technical and Organizational Measures): GDPR Article 32 requires controllers and processors to implement appropriate security. Section 3 of this document ("Security Measures") will detail our technical measures, but in summary, we apply strong encryption, access control, and have an information security management program that covers risk assessments and regular testing of our defenses. Organizationally, Tekle has a security team and a privacy officer (or team) overseeing compliance. Confidentiality is built into employee contracts, and we limit access to personal data strictly on a need-to-know basis. If we ever experience a personal data breach, we have a procedure to notify the controller without undue delay (we aim for well under the 72-hour window given by GDPR for controllers to notify authorities, so we typically notify within 24 hours of confirmation of a breach, providing as much detail as available).

Record-Keeping and DPIAs: Tekle maintains a Record of Processing Activities (RoPA) as required by GDPR Article 30, documenting what personal data we handle, the purposes, data subjects, etc. We also perform Data Protection Impact Assessments for any new or changed processing that might be high risk (e.g., if we introduced a feature that uses personal location data, we'd conduct a DPIA to ensure we mitigate any privacy risks).

International Data Transfers: Tekle's default approach is to process data in the region of the customer to avoid unnecessary data transfers. However, our company does have team members and sub-processors outside of the EU (for example, our support team might access a system from our office in the Netherlands or, if we have US support staff for US clients, from the US). For any EU personal data that flows to a country without an adequacy decision (like the US), we rely on **Standard Contractual Clauses (SCCs)** as our transfer mechanism, appended to our DPA. We have additionally reviewed our transfers in light of the Schrems II decision – for instance, for EU->US transfers, we have assessed the risk of US government access to data and found it low given the type of data we handle (primarily business data). We still implement additional measures such as encryption of data in transit and at rest (with keys managed in the EU for EU data) which adds an extra layer of protection. We are monitoring the implementation of the new EU-US Data Privacy Framework; if it becomes a valid mechanism and provides more assurance, we may incorporate it for relevant transfers.

Other Jurisdictions: Outside of GDPR, we comply with other data protection laws as applicable:

- **United States (CCPA/CPRA):** While Tekle primarily serves enterprises, if any personal data falls under the California Consumer Privacy Act or its amended version CPRA, we handle it in accordance. We do not "sell" personal information as defined by CCPA. We treat ourselves as a "Service Provider" when dealing with customer data, meaning we only use personal info to provide the service and not for secondary purposes. We support customers in responding to California residents' rights similar to GDPR processes.

- **Canada (PIPEDA):** We follow similar principles of consent and safeguarding for any data on Canadian individuals, and would comply with any access requests under PIPEDA.

- **Asia-Pacific:** Tekle follows the Singapore PDPA and Australian Privacy Act principles when relevant, ensuring consent and providing access/correction rights. We also comply with Japan's APPI for any Japanese personal data (e.g., we would treat certain identifiers as "personal information requiring special care" appropriately).

- **Other EU Regulations:** We comply with the ePrivacy Directive in contexts where it applies – for example, our website's use of cookies is minimal, and we provide cookie opt-outs. Our products themselves do not engage in electronic communications in a way that implicates ePrivacy (they aren't sending direct marketing or using cookies beyond standard web interface sessions).

- **Data Retention:** Tekle's policy is to retain personal data only as long as necessary. For active customer accounts, we retain data for the duration of the contract. After contract termination, unless instructed otherwise, we will delete personal data within a defined period (typically 30-60 days after termination). If some data must be retained for legal obligations (e.g., transaction records for accounting), we archive it securely for the required period then delete. We include these retention commitments in contracts so there's a clear understanding.

Data Protection Agreements with Customers: We fully expect to sign a Data Processing Agreement with any customer who provides us personal data. Our standard DPA is included, but if a customer has their own template DPA or particular clauses they need (perhaps referring to specific national law implementations or additional safeguards), we review and accommodate them so long as they don't conflict with our ability to provide the service. Typically, there is little issue here as our interests align (protect the data and comply with law).

Sub-Processors: Transparency about who else might process your data is important. Tekle maintains a sub-processor list. For example, our primary sub-processor is Microsoft Azure (as an IaaS/PaaS provider). We might also use a service like SendGrid to send notification emails (meaning if we send an alert email to a user, that user's email passes through SendGrid, which is a sub-processor). All sub-processors are bound by data protection terms equivalent to our DPA (we have SCCs in place with those outside the EU). We inform customers via our Trust Center online about any new sub-processor at least 30 days in advance, giving the opportunity to object. To date, our sub-processor list is short and consists of well-known, reputable providers.

Privacy by Design Examples: To illustrate Tekle's commitment, consider how we designed our collaboration feature. When multiple users collaborate on a holographic model in the cloud, each user's device shares their viewing perspective and any annotations they make. Rather than sharing any personal identifier, the system uses session-based IDs and only the data necessary to sync the experience (like positions, comments). If an audit trail is needed, we log user IDs for the session, but those user IDs are internal (like an employee number or username) and we don't expose them beyond the customer's own admin view. We also implemented a feature where an admin can enforce pseudonymous mode, meaning in multi-user sessions users see generic labels (like "User 1") instead of personal names, if anonymity among participants is desired for study or privacy reasons. These are small examples but showcase that we actively think about minimizing unnecessary personal data exposure.

ITAR and Defense-Related Compliance

For our customers in the defense and aerospace sectors, compliance with defense regulations and safeguarding sensitive military information are non-negotiable priorities. Tekle Holographics has established protocols to ensure that we comply with **International Traffic in Arms Regulations (ITAR)** and other relevant standards when handling defense-related projects.

ITAR Overview: ITAR governs the export of defense-related materials and technical data as listed on the United States Munitions List (USML). Even though Tekle is based in the Netherlands, ITAR can apply to us if, for example, we deal with technical data from a U.S. defense customer or if our products are used to develop or produce defense articles. Non-U.S. companies can comply with ITAR by implementing equivalent controls to prevent unauthorized foreign access and by obtaining export licenses through U.S. partners when needed.

Our ITAR Compliance Measures: Tekle's approach to ITAR can be summarized in a few key points:

- **US Persons and Facilities:** If an ITAR situation arises (say, a U.S. defense client wants to upload ITAR-classified schematics into a Tekle system for visualization), we ensure that only **US Persons** (U.S. citizens or permanent residents) employed or contracted by Tekle handle that data. To facilitate this, Tekle has a partnership with a U.S.-based entity (or subsidiary) that can employ US Persons with the appropriate clearances. We either route support for that client exclusively through those authorized individuals or have them sign NDAs and Technology Control Agreements limiting access to others. Additionally, we are prepared to host the client's data on U.S. soil – we can deploy their instance in an isolated U.S. data center, possibly using a GovCloud environment if required. This way, data doesn't transit through foreign systems.

- **Technology Control Plan (TCP):** Tekle has developed an internal Technology Control Plan for ITAR. The TCP outlines how we identify ITAR-controlled technical data, how we mark and handle it, and the security measures in place. It covers physical security (like segregated ITAR project folders accessible only to cleared personnel, ITAR data labeled accordingly), information security (encryption and access logs for ITAR files, separate ITAR-only communication channels with clients), and personnel screening (verifying citizenship status of anyone who will work on the project).

- **Licensing and Approvals:** If Tekle needs to receive ITAR technical data from a customer or send any to a colleague, we work with the customer to ensure a **DSP-5** export license (for technical data exports) or other necessary approvals are in place. Often the customer (as the owner of the data) will sponsor and secure the license naming Tekle (and any relevant personnel) as authorized recipients. We have legal counsel familiar with ITAR to advise on these matters, and we do not proceed until all paperwork is in order. For example, before a U.S. aerospace client provided us with an ITAR-controlled CAD model to visualize on a Holo-Table, we were added to their Technical Assistance Agreement (TAA) with the U.S. State Department, legally authorizing us to handle that model.

- **EAR and Dual-Use:** While ITAR is about defense, the Export Administration Regulations (EAR) cover dual-use technologies. Some components of Tekle's hardware could be considered dual-use (though mostly they are commercial). We classify our products and have determined most fall under EAR99 or a non-sensitive ECCN (Export Control Classification Number). Nonetheless, we remain vigilant. If a customer project involves controlled dual-use tech (like certain encryption or aerospace data under EAR), we treat it with similar caution and comply with licensing if shipping hardware or software to restricted countries.

- **DFARS/NIST 800-171 Compliance:** U.S. defense contractors often require compliance with cybersecurity standards like NIST SP 800-171 or the Cybersecurity Maturity Model Certification (CMMC) for protecting Controlled Unclassified Information (CUI). Tekle aligns with these requirements for relevant projects. For instance, if we store CUI (which could include technical drawings or data not classified but sensitive), we implement the 110 security controls of NIST 800-171: multi-factor auth, strict access controls, incident response plans specifically addressing CUI, media protection, etc. Many of these controls overlap with what we already do (encryption, logging, training). We can provide a controls matrix mapping our practices to NIST 800-171 upon request, to demonstrate our capability to protect CUI.

- **NATO and Other Standards:** For clients in NATO countries or other alliances, similar principles apply. We handle NATO classified or restricted info only if we have the clearance and need; currently Tekle does not directly hold facility clearance for classified info, so we usually deal with unclassified-but-sensitive data, but with ITAR-level handling if needed. If in the future we pursue such clearances, we will update our compliance documentation.

Audit and Certification: If a defense client wishes to audit our ITAR compliance measures (or broader security) through a site visit or inspection, Tekle is open to that under appropriate confidentiality terms. We maintain documentation (like the Technology Control Plan, training records for staff on export control, logs of data access) that can be reviewed to verify compliance. Thus far, we have passed customer audits which checked our handling of their sensitive data.

Employee Training and Awareness: All relevant Tekle employees undergo training on export controls annually. This training covers the basics of ITAR/EAR, recognizing ITAR-controlled technical data, the severe penalties for violations, and our internal procedures. We emphasize a culture of "If in doubt, ask" – employees are instructed that if they suspect data might be export-controlled and they aren't sure of their authorization, they should halt and consult our compliance officer before proceeding.

Tekle can confidently engage in defense projects by building a framework that mirrors the stringent requirements of the defense industry. Clients can trust that we won't inadvertently expose controlled data, and that we take the legal responsibilities as seriously as they do. This compliance mindset also benefits all customers, because the rigors of defense-grade security elevate our overall practices.

Technical Security Measures (Summary of Controls)

(Note: This section may recap some info from the Security Architecture document but focuses on listing key measures for compliance documentation purposes.)

To provide a clear overview for compliance review, below is a summary list of Tekle's key technical and organizational security measures:

- **Physical Security:** Data centers hosting Tekle Cloud are protected by multi-layer physical security (24/7 guards, CCTV, biometric access, fire/flood controls) through our IaaS providers. Tekle's office and any location where data might be handled have access controls (badges), visitor logs, and secure disposal bins for sensitive printouts (though we are largely paperless). Devices shipped from Tekle are sealed and tested for security.

- **Access Control:** Role-based access both in product (for users) and internally (principle of least privilege). Strong authentication (password policies, MFA enforced for admin roles). Unique user IDs – no shared accounts in operations. Timely removal of access when personnel change roles or leave. Customer data access by Tekle staff only via support process with logging.

- **Data Encryption:** AES-256 encryption at rest for all databases and storage. TLS 1.2+/HTTPS for all data in transit. Encryption keys managed with restricted access and rotated periodically. Option for client-managed keys available for certain deployments if required (we can integrate with a customer's Key Management Service if they want full control).

- **Network Security:** Firewalls and security groups segment our network. Only necessary ports open, and only between necessary components. Use of VPN for any remote admin access. IDS/IPS and anomaly detection on network traffic. DDoS mitigation services enabled. No direct exposure of databases to the internet; all access goes through application layer.

- **Application Security:** Secure development lifecycle as detailed earlier – code review, scanning, pen-testing. Web application firewall (WAF) in front of any web endpoints to catch common attacks (SQLi, XSS). Regular vulnerability patching.

- **Endpoint and Device Security:** Tekle devices (like Holo-Table) run on a hardened operating system image (unneeded services removed, host firewall on). Anti-malware and application allow-listing in place. The devices can be set to kiosk mode to prevent general OS usage. Ports/IO on devices can be disabled or enabled per client preference (for instance, USB ports can be locked down via policy if concerned about unauthorized use).

- **Logging and Monitoring:** Centralized logging of security events. Automated alerts for critical events. Daily review of security reports. Retention of logs as per policy (e.g., 1 year online, additional year archived). Integrity protection for logs.

- **Backup and Recovery:** Databases are backed up daily (with transactional log backups more frequently). Backups encrypted in storage. Recovery tested periodically. For on-prem customers, backup procedures are provided and can be automated via our tools (e.g., an admin can schedule exports of project data).

- **Business Continuity:** Redundant architecture for cloud services, failover capability. Documented DR plan with RTO/RPO objectives. Key staff have emergency access to needed tools from remote locations to manage incidents if offices are unavailable.

- **Organizational Measures:** Security and privacy training for all staff annually. Security awareness (phishing tests, newsletters). Incident response team and plan, as described. Vendor risk management program (ensuring our sub-processors meet standards). Confidentiality agreements with employees and contractors.

Each of these measures maps to controls expected in frameworks like ISO 27001, SOC 2, or NIST CSF, and demonstrates Tekle's holistic approach to protecting data.

Contractual Commitments and Compliance Support

Tekle's contractual documents reflect the measures and commitments described:

- Our **Data Processing Agreement (DPA)** legally commits us to the GDPR-aligned measures (like assisting with rights, breach notification, etc.) mentioned above.
- The **Master Service Agreement (MSA)** contains warranties that we have and will maintain appropriate security measures and comply with applicable laws (including data protection laws). It also addresses liability sharing in case of data breaches (we typically accept liability for breaches caused by our negligence, subject to agreed caps).
- If a client requires specific compliance clauses (for example, for HIPAA in healthcare, if one of our solutions were used for patient data, we would sign a Business Associate Agreement and follow HIPAA security rules), Tekle is open to that and capable of meeting those standards as well.
- We also include commitments to compliance with anti-corruption laws (UK Bribery Act, FCPA) and environmental/equality regulations in our corporate policies, which, while not directly related to data security, often form part of the overall compliance picture enterprises consider in trust centers.

Tekle Holographics is not only an innovator in holographic visualization but also a responsible custodian of data and a compliant partner for regulated industries. This Data Protection & Compliance Overview has detailed how we embed privacy and compliance into our operations – from following GDPR's stringent requirements to handling ITAR-controlled data with care. We invite clients and auditors to review our policies and even test our practices; we believe in accountability and are confident that our dedication to compliance will meet your organization's standards.

For any questions about our data protection approach, or to request documents like sub-processor lists, audit reports, or mappings of our controls to specific regulations, please contact our Data Protection Officer or your Tekle account representative. We are here to ensure that adopting Tekle's technology also means enhancing, not ever compromising, your compliance posture.