Data Compliance

Foundation of Data Compliance

Procurement and supplier data must be treated as a strategic asset, just as customer data is. Mishandling procurement data can create regulatory exposure, lead to fines, and undermine contractual obligations with suppliers. Procurement data must be maintained under strict data compliance requirements, ensuring alignment with legal, regulatory, and industry standard efforts associated with enterprise-grade data management, transfer, and governance across all relevant geographies.

Levelpath demonstrates adherence to applicable laws, regulations, industry standards, and contractual obligations across jurisdictions. From a legal standpoint, this reduces the risk of penalties for clients by showing that proper care has been taken to respect both local and international requirements. From a compliance perspective, Levelpath's rigorous due diligence and internal controls reduce the risks of regulatory non-compliance, while also providing evidence of good-faith efforts in the event of a dispute or investigation associated with the supplier relationships, contractual management, and sourcing activities that are managed in the platform.

All client AI data is safeguarded under enterprise-grade licenses, with encryption applied both at rest (AES-256) and in transit (TLS 1.2 or 1.3, as appropriate).

These technical safeguards matter because regulators such as those enforcing GDPR, HIPAA, and PCI DSS require organizations to use "appropriate technical and organizational measures" to secure personal and sensitive data. Encryption provides a legal defense by demonstrating proactive mitigation of confidentiality and integrity risks.

Privacy Governance

Levelpath maintains transparent external legal documents, including Terms of Service, a Data Processing Addendum, and a Privacy Policy that explicitly define user rights and obligations. From a data compliance perspective, these instruments are essential to fulfilling legal transparency obligations under privacy laws worldwide. They also form the contractual foundation for the enforcement of data rights between Levelpath and its clients.

As an example, GDPR (General Data Protection Regulation) legally enforces the rights of European Union residents to access, correct, and erase data, mandates breach notification within 72 hours, and requires data minimization. Compliance with GDPR demonstrates accountability and reduces exposure to severe fines of up to 4% of global revenue.

Activity-Based Governance

Operational safeguards are demonstrably aligned with SOC 2 Type II, which requires continuous evidence that controls are in place to secure and manage data responsibly. Levelpath provides comprehensive audit logs and compliance evidence to regulators and independent auditors. Audit logs and SOC 2 Type II validation provide critical proof of data compliance, demonstrating accountability to regulators and auditors. This matters because:

- **From a legal perspective:** the ability to show complete audit trails and logs demonstrates "accountability" in line with GDPR, SOX, and other statutes requiring documented proof of controls.
- **From a regulatory compliance perspective:** Levelpath's independent audit validation reduces liability exposure by showing that internal processes have been third-party tested and verified against recognized standards.
- **From a procurement governance perspective:** these audit logs allow clients to meet internal audit requirements when regulators demand evidence of proper data handling across the supply chain.

Data Protection and User Rights

Customers are granted rights to access, correct, delete, and port their data, aligning with GDPR and other data privacy requirements. The recognition and enablement of these rights matters legally because failure to honor them can trigger enforcement actions, civil penalties, or legal claims.

Breach notification processes are established to meet time-bound regulatory mandates globally, such as GDPR's 72-hour requirement. Timely notification matters legally because delayed disclosure can increase fines and reputational damage, while timely compliance demonstrates responsibility and reduces liability.

Subprocessors and suppliers are thoroughly vetted for compliance. From a legal standpoint, organizations are responsible for the conduct of their processors under a variety of data protection laws. By publishing an up-to-date subprocessors list and executing standardized Data Processing Agreements (DPAs), Levelpath provides transparency and accountability that reduces the risk of liability for hidden third-party practices and ensures clients can meet their own obligations to regulators.

Global Assurance

Levelpath's data compliance efforts align with global frameworks such as GDPR, ensuring that customers benefit from consistent, enforceable protections. This matters legally because it demonstrates a baseline compliance posture that can apply to local requirements without negotiating separate protections for each jurisdiction.

From a compliance perspective, this approach reduces audit complexity and operational overhead for procurement teams by allowing procurement organizations to rely on a unified compliance standard to lower both regulatory and contractual risk exposure.

For additional information on Levelpath's Data Compliance efforts, please visit the following sites:

- Data Processing Addendum
- Privacy Policy
- Security
- Terms of Service
- Trust Center

Keep your data compliant with Levelpath.

Request a demo.