Levelpath Data Governance

Levelpath is an AI-native platform designed to ensure data integrity, security, and compliance while enabling procurement efficiency. From a governance perspective, customer data is always treated as an enterprise asset that belongs solely to the client. Levelpath provides application functionality and AI-driven execution without compromising ownership, control, or compliance.

Every interaction with intake workflows, contract management, supplier management, supplier risk analysis, and invoicing aligns with enterprise requirements for encryption, ownership, and regulatory standards. Our commitment is to safeguard enterprise, supplier, financial, and contractual data across its lifecycle, ensuring it remains protected, controlled, and auditable. Governance practices cover sourcing, contracts, supplier management, supplier risk, and invoicing.

Technical Data Security

Levelpath enforces strict safeguards that prevent misuse, ensure accountability, and align with enterprise compliance standards by guaranteeing client ownership of all data, applying granular access policies, integrating with enterprise authentication systems, separating duties across workflows, and maintaining immutable audit trails. These measures ensure that data remains protected, auditable, and under the client's direct control at all times.

- **Customer Ownership:** Levelpath clients retain full ownership of their data at all times. Data is never used to train third-party software or models and remains under client stewardship.
- **Granular Access:** Role-based and attribute-based access controls (RBAC and ABAC) ensure that only authorized personnel in procurement, finance, legal, or related functions can access specific data sets.
- **Authentication:** Single sign-on (SSO) is the standard authentication model, integrated with enterprise identity providers. Verified users are mapped to the appropriate teams and roles according to enterprise protocols.
- **Segregation of Duties:** Supplier onboarding, sourcing events, and contract approvals are designed with separation of responsibilities. Legal, IT, security, procurement, and other stakeholders have defined workflow roles that enforce compliance and minimize risk.
- **Audit Trails:** All activities are tracked through immutable logs, including user actions, administrative changes, approvals, and workflow events. These logs support visibility and accountability across procurement processes.

Data Privacy and Protection

Levelpath embeds privacy into its architecture and operations, enforcing strong encryption, logical segregation of environments, and compliance with global data protection regulations. By building privacy controls into the platform by design, Levelpath ensures that sensitive information remains confidential, accurate, and compliant with regulatory frameworks.

- **Encryption:** Data in transit is encrypted using TLS 1.2 or 1.3, while data at rest is encrypted with AES-256.
- **Data Segregation:** Levelpath's multi-tenant architecture enforces logical separation between customer environments to prevent unauthorized access or data leakage.
- **Privacy by Design:** Privacy is embedded into the platform. Levelpath complies with GDPR, CCPA, and other data protection frameworks and provides a standard Data Processing Agreement (DPA) to support client-specific compliance needs.

Compliance and Certifications

Levelpath aligns its controls with leading standards such as SOC 2 Type II and GDPR while also supporting contractual governance through integrations with eSignature and contract management processes. Ongoing penetration testing and vulnerability assessments reinforce the platform's resilience and demonstrate a commitment to continuous compliance.

- **Security Standards:** Levelpath holds SOC 2 Type II certification, demonstrates GDPR readiness, and supports client-specific protection standards.
- **Contractual Compliance:** The platform integrates with enterprise eSignature solutions and supports client-defined contract record policies.
- **Independent Testing:** Penetration tests, vulnerability assessments, and third-party audits are conducted regularly and after major functional updates to ensure resilience.

Data Lifecycle Management

Levelpath data governance aligns lifecycle management with legal and financial standards by ensuring accurate supplier onboarding with resilient cloud-based storage, configurable retention periods, and verified deletion procedures. Levelpath reinforces customer ownership and makes data fully portable across systems with open APIs and native connectors in full compliance with client and industry standards.

- **Supplier Onboarding:** Supplier and contract onboarding processes follow client-based validation standards, including metadata extraction and enrichment of records.
- **Data Storage:** Data is stored in an encrypted, resilient public cloud infrastructure with multi-domain and multi-tenant deployments that preserve logical separation.
- **Record Retention:** Retention policies are configurable to align with financial and compliance requirements, such as seven years for invoices.
- **Client Right to Data Deletion:** Customer-owned data can be securely and verifiably deleted upon request or contract termination.
- **Record Portability:** Supplier records, contracts, and invoices can be exported through REST APIs, webhooks, or native connectors to ensure portability and ownership.

Supplier and Third-Party Handling

Levelpath applies rigorous due diligence to all subprocessors, enforces contractual agreements through a Data Processing Agreement, and discloses relationships transparently. Supplier sustainability, diversity, and risk information is managed with the same governance and rigor, ensuring that enterprises can meet compliance obligations.

- **Third-Party Risk Management:** All subprocessors undergo due diligence before engagement, with continuous monitoring thereafter.

- **Data Sharing:** Client data is shared only with approved subprocessors under DPAs. Subprocessor relationships are disclosed transparently.
- **ESG and Risk Data:** Supplier sustainability, diversity, and risk assessment data are securely managed, with controls that align with enterprise and regulatory standards.

Monitoring, Incident Response, and Business Continuity

Levelpath delivers continuous monitoring across the platform with integrated anomaly detection, documented incident response playbooks with clear escalation paths, and service-level commitments. Redundant infrastructure, tenant-level isolation, and tested disaster recovery procedures ensure resilience to ensure that procurement and supplier processes remain available, secure, and compliant.

- **Continuous Monitoring** The platform is monitored 24/7 using anomaly detection and SIEM systems. Log management ensures activities are captured and available for review.
- **Incident Response:** Levelpath maintains incident response playbooks with SLAs for detection, escalation, and notification. Uptime SLAs define how issues are triaged and resolved.
- **Business Continuity:** The SaaS architecture employs logically separated databases, customer-specific encryption keys, and role-based controls. Redundant infrastructure, automated failover, and tested disaster recovery procedures support uninterrupted operations. SOC 2 controls and access audits validate resilience and data isolation.

Governance Organization and Policies

Levelpath data governance is reinforced through formalized security, privacy, and anti-fraud requirements, with employees receiving regular training in least-privilege access and secure data handling. As part of this policy, Levelpath has a Data Protection Officer to align governance practices with evolving regulations such as the EU Data Act and EU AI Act. Transparent documentation and support for audits or regulator inquiries ensure that governance is not just policy, but an operational practice.

- **Data Oversight:** A GDPR-compliant Data Protection Officer (DPO) oversees governance activities with support from cross-functional teams across IT, compliance, procurement, and finance. Practices align with evolving requirements such as the EU Data Act and EU AI Act.
- **Security and Retention Policies:** Formal policies cover information security, privacy, acceptable use, and retention requirements. At Levelpath, these policies are reviewed and updated regularly.
- **Employee Training:** Employees receive recurring training on least-privilege access and secure handling of supplier, payment, and contract data.
- **Transparency:** Clients receive structured documentation and support for audits, questionnaires, and regulator inquiries, with both scheduled and platform-based reviews available.

Customer Rights and Transparency

Levelpath affirms that customers own their information and can access, review, or export data at any time. Dashboards provide visibility into data flows and subprocessor relationships, while published disclosures clarify third-party engagement. Levelpath also assists customers during regulatory reviews, enabling enterprises to demonstrate compliance confidently.

- **Data Access:** Customers can request, review, or export their data at any time.
- **Transparency Dashboards:** Dashboards provide visibility into data flows, subprocessors, and compliance posture. Subprocessor lists are maintained and disclosed.
- **Regulatory Engagement:** Levelpath supports clients during regulator inquiries, including GDPR, SOX, and other industry-specific requirements, ensuring full compliance across Levelpath-managed data.

Recommendations

Data governance is a business practice that ensures enterprise resilience, regulatory alignment, and stakeholder trust. To support this, Levelpath data governance prioritizes clear ownership of information, strict access controls, verifiable privacy protections, and transparent accountability across every stage of the supplier and contract lifecycle. In this light, Levelpath provides the following recommendations to procurement professionals:

1. **Position procurement as active stewards of enterprise data, working in conjunction with digital, data, and AI executives.** – To elevate procurement's role in enterprise governance and risk management, sourcing and procurement pros must treat procurement data with the same rigor as financial or customer records.
2. **Embed access and privacy controls into core workflows.** – Procurement should not just bolt-on compliance at the beginning, but should embed privacy and access controls directly into supplier onboarding, sourcing, and contract approval workflows. Role-based and attribute-based access, single sign-on authentication, and immutable audit trails should be operationalized across procurement workflows so compliance is automatic, not optional.
3. **Modernize procurement data lifecycle management.** – Executives should define lifecycle policies from onboarding through retention and verified deletion. Supplier and contract records must be portable to ensure long-term flexibility while being resilient through encrypted cloud storage and tested recovery processes. Treating lifecycle management as a strategic function strengthens trust and ensures readiness for audits or transitions.
4. **Extend governance to supplier and third-party ecosystems.** – Procurement executives must enforce governance standards across third-party data and supplier-provided information (such as ESG, risk, and compliance records). Contracted subprocessors must adhere to contractual privacy obligations, data flow transparency, and supplier diversity and sustainability data into risk frameworks.
5. **Prepare procurement data for an AI-native future.** – AI-driven procurement will depend on clean, compliant, and well-governed data. Executives should prioritize privacy-by-design approaches, ensure regulatory alignment with evolving frameworks such as the EU AI Act, and invest in transparency dashboards that give visibility into how procurement data is stored, processed, and shared. By laying this groundwork, procurement teams can confidently adopt AI tools for sourcing, negotiation, and risk management without compromising security or compliance.
6. **Assess readiness for enforcing data governance across workflows.** – Ensure that roles and permissions are defined, privacy frameworks are embedded, and monitoring and continuity are tested in practice. Procurement data cannot be ignored after intake; data and relevant documents must be managed and governed throughout the workflow. Platforms that cannot answer these questions expose enterprises to operational, financial, and reputational risk.

Conclusion

Levelpath positions governance as a strategic enabler for the procurement department. The platform safeguards enterprise data, supplier information, and financial records. It also gives customers the transparency and assurance to meet internal policies, satisfy regulatory obligations, and maintain executive confidence. This approach enables IT, compliance, and procurement leaders to advance digital transformation with the certainty that sourcing, contracting, and supplier interactions are governed at an enterprise level.

For additional information on Levelpath Data Governance, please access Levelpath's publicly available commitments to data security, privacy, and trust:

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