Frequently Asked Questions

Contents

Certifications

- What independent audit reports and certifications are available?
    - The following Group organizations complete annual audits and have ISO 27001, ISO 27701 and SOC 2 type 2 certifications/reports:
        - Affirmity
        - Breezy
        - Bridge
        - Gomo
        - Open LMS
        - PeopleFluent
        - Rustici
        - Watershed
    - In addition to the above we are aligned with ISO 42001, establishing an AI Management System to provide assurance we are following an established and internationally recognised standard in managing AI.
- How do I obtain a copy of your SOC 2 report or ISO certificates?
    - The ISO 27001 & ISO 27701 (Privacy) Certificate can be downloaded from our Trust Center. We are happy to share our SOC 2 report with relevant parties; however, mutual NDA and confidentiality terms apply. To obtain a copy of our SOC report, please complete the form on our Trust Center.
- Does the Company hold cyber liability insurance?
    - Yes. Details of the Company's cyber liability insurance can be shared under NDA. Contact your Account Representative for assistance.
- Do you conform to a specific industry standard security framework?
    - Company's security controls and policies are derived from industry data security and privacy best practices such as OWASP, ISO-27001, NIST, and SANS guidelines

Data Privacy

- Where is your Privacy Policy?
    - The Privacy Notice can be found here: https://ltgplc.com/privacy-notice/
- How is privacy handled?
    - We have an ISO 27701 certified Privacy Information Management System (PIMS). We are compliant with all major privacy frameworks such as GDPR and CCRA.
    - You can find our Data Privacy Framework Certification by going to https://www.dataprivacyframework.gov/list and searching 'Learning Technologies Group'. For more information please enquire via privacy@ltgplc.com.
- I would like you to remove my personal information from all of your systems. How do I request this?
    - If your personal information was collected by a company using one of our service offerings (for example, if one of our customers is your employer, and your employer collected this information using our services), then you should contact that company directly regarding your request.
    - If your personal information was collected by us, you may submit your request using our Data Subject Request Form.
- How is my data handled?
    - Formal Data Classification Policy is part of the Information Security Management System (ISMS). Client data is uniformly classified as the highest level of data sensitivity.
    - All client data is handled as Restricted, the highest level of sensitivity regardless of content. PCI, PHI, and PFI are prohibited data categories on our systems.
- What are the Company's and Client's respective roles under the DPA with regards to GDPR?
    - The Company acts as a Data Processor on behalf of our Clients. The Client is the Data Controller.
- Can the Company sign a Client's DPA?
    - No. The Company's DPA is tailored to the services we provide and reflects our product architecture and organizational process. These processes are standard across our organization and products and are not customized or configurable by individual customers. Our online DPA is available here: https://ltgplc.com/data-protection-addendum/
- Do you share our data with any third parties?
    - Data is not shared with third parties other than our sub-processors that are necessary to provide our services. A list of our sub-processors can be found https://ltgplc.com/sub-processor-list/
- Do you retain our data after using your services?

- No, data is removed from active systems shortly after our relationship ends. This is usually either 30 days after a contract end date, or if applicable, 30 days after any services data export engagement is concluded. In some cases encrypted backups of data may be retained for up to 13 months at which time they are securely destroyed per our backup retention policy.

Sub-Processors

- Does the Company use sub-processors?
  - See our Sub-Processors List.
- Does the Company have a DPA in place with Sub-Processors?
  - Yes, see our Supplier Data Processing Agreement.
  - Also see our *Vendor Management Policy* for additional details regarding our Third-Party Vendor Management Program, available via the Trust Center.
- Does the Company notify Clients of new Sub-Processors in advance?
  - Yes, see the Data Protection Addendum for details.
  - Additionally, notification details are outlined on the Sub-Processor List.
- What measures secure your supply chain/vendors?
  - Vendor risk assessments are completed prior to onboarding and annually thereafter on all our vendors to ensure that their security capabilities align with our standards and commitments. For more information on this process you can find the *Vendor Management Policy* on the Trust Center.

Policies & Procedures

- Where can I find your security policies?
  - Our public-facing policies can be found on our Trust Center.
- Do you complete background screenings of employees?
  - During the hiring process we perform References and Employment Verification, Criminal Background Check (where allowed), Proof of Citizenship/Right to Work, Social Security Number Crosscheck, and OFAC list check.
- Are segregation of duties enforced when developing, testing and deploying code?
  - Yes. The Company has in place segregation of duties and responsibilities based on job roles. Only designated personnel have the accesses necessary to deploy code via automated processes. Neither core development personnel nor QA can deploy code to production systems.
- Where can I find out more about encryption?
  - Our *Data Encryption Policy* references data in transit and rest, email encryption and transfer protocols. To learn more about key management,

please see our *Encryption Key Management Policy* available via the Trust Center.

- Describe your security incident response process.
  - The Company has formal Security Incident Handling Procedures that are tested annually. The security incident response process defines the stages of the incident life cycle (including Preparation, Detection, Observation & Containment, Resolution & Recovery, and Post-Mortem & Continuous Improvement); ensures appropriate engagement of cross-functional stakeholders, executive management, and specialized external resources; ensures that the company fulfills all legal, regulatory, and contractual notification requirements.
- Do you test your incident response plan?
  - Yes, the incident response plan is tested at least annually to ensure relevant stakeholders are well prepared to fulfill their responsibilities and to identify improvement opportunities for the plan.

Disaster Recovery

- What are your recovery time objectives (RTO) and recovery point objectives (RPO)?

Business Unit	RTO	RPO
Breezy	72 hours	24 hours
Affirmity, Bridge, Gomo, Instilled, Open LMS, PeopleFluent, Reflektive	72 hours	2 hours
Rustici, Watershed	4 hours	24 hours

- How often are the Business Continuity and Disaster Recovery Plans tested?
  - The BCP and DRP are reviewed and tested at least annually. Results validate the effectiveness of our continuity/resilience controls.
- Can I get a copy of your results from the last BCP/DRP test?
  - Due to the sensitive nature of these plans, we are not able to provide details of the annual test exercise, nor any improvements made as a result of the exercise. We can only provide attestation of when the last exercise was completed and confirmation of the alignment of test results with recovery objectives.

Security

- Do you provide information security and privacy training?

    - Yes, training is conducted annually and as part of the onboarding process. The training is reviewed annually and it includes a knowledge test component to ensure competency.
    - In addition to security awareness training, all technical personnel are required to complete continuing technical security training annually
- What Technical and Organizational Security Measures does the Company have in place?
    - See Appendix II of the DPA: https://ltgplc.com/data-protection-addendum/
    - The Company also undergoes a SOC 2 Type II audit annually, which attests to the controls governing the availability, confidentiality, and security of Client data.
- How is access and identity controlled?
    - We use a combination of role-based access controls (RBAC), zero-trust access controls, regular access reviews, SSO/MFA enforcement and least-privilege principles.
- What logs do you keep and how long for?
    - Please see our Data Retention, Destruction and Disposal Policy available on our Trust Center.
- Can Clients conduct penetration or vulnerability testing?
    - No. Client driven security scans, security testing, and any form of penetration testing is expressly prohibited. The Company performs comprehensive security testing and vulnerability management and makes relevant assurance documentation available to its clients upon request through its independent security audit and certification programs.
    - We engage a specialized third-party to perform our penetration tests to independently validate system security. An executive summary of the penetration test results is available to Clients upon request.
- We recently heard about a new vulnerability. Is our system vulnerable?
    - We have a comprehensive vulnerability management process in place to monitor for and address new vulnerabilities as they arise. You can be confident that we are aware of relevant vulnerabilities as they are disclosed publicly and taking appropriate actions with due urgency. For more information, see our Vulnerability Management Policy. Also keep in mind that vulnerability information is highly sensitive, so we will not

Additional Questions? Reach out to your Account Representative or contact us at compliance@ltgplc.com