G3 Translate

Policy for the Protection of Personal Data

It is the highest priority of G3 Translate to ensure that any project content submitted to us remain secure, private and confidential. This policy regards the treatment and protection of personal data by G3 Translate in the performance of the services it provides. You or your company may be parties to one or more agreements for translation, transcription and/or related services that may involve, on an incidental basis, the presence of personal data. The content of any files submitted by you or your company (Client) to G3 Translate (G3) will remain the sole property of the Client, and will not be used for any purpose other than those agreed to by the Client and G3 for the execution of the services requested.

This policy applies to personal data collected by the Client and processed by G3. It does not apply to the personal data of the Client or representatives of the Client collected by G3.

Client is hereby informed that the principle purpose of the services provided by G3 is not the processing of personal data and that the presence of any personal data in processed files is infrequent and of uncommon occurrence in the execution of services provided. Client is further advised that, per the terms of service of any existing agreement, G3 may not possess the means to access the personal data, and may be unable to identify the data subjects or the personal data that may be in need of protection.

Personal data in files to translate or transcribe:

a) If Client receives from their end client files that contain personal data, Client's role shall be that of Processor, and G3's role shall be that of Sub-Processor. In such case, the data controller is the end client of the Client.

b) G3 may not be aware of the presence of protected personal data in the files unless Client explicitly informs G3 of same. In such case, the responsibility of protecting such Client personal data remains with Client.

c) Client is requested to remove personal data from files or replace said personal data before sending them to G3 for processing, whenever it is possible that such personal data can be removed, replaced with pseudonyms or rendered anonymous.

Data Sharing/Sub-Processing

The nature of Services provided to Client by G3 are such that the engagement of Sub-Processors may be required. G3 shall do each of the following:

a) perform adequate due diligence on each Sub-Processor such that said Sub-Processors provide sufficient guarantees to implement measures to ensure that the processing of personal data will meet the basic requirements of applicable Data Protection Laws;

b) stipulate terms in the contract between G3 and each Sub-processor that are the same as or substantially similar to those set out in this policy. Upon request, G3 shall provide a copy of its agreements with Sub-Processors to Client for its review.

c) remain liable to Client for any failure or breach by a Sub-Processor to fulfill its obligations in the processing of personal data.

Rights of Data Subjects

G3 shall execute appropriate measures to assist Client in its obligation to satisfy requests by data subjects to exercise their rights of access, modification or erasure, to restrict or object to processing of personal data. Requests for the removal of personal data may be made to info@g3translate.com or by calling 212-889-5077 and requesting to speak with the Data Privacy Officer.

Compliance Audit

Upon reasonable written request from the Client, G3 will permit Client to perform an audit related to the processing of personal data to verify compliance with the requirements for the protection of personal data.

Personal Data Security

Processor will implement organizational and technical measures to ensure a level of security to protect against the risk of unauthorized or unlawful processing of personal data, and of accidental loss, unauthorized disclosure, alteration, damage to, or destruction of, personal data.

In the event of a personal data breach, G3 will promptly notify Client of same in order to permit Client to fulfill reporting obligations of said breach under applicable Data Protection Laws. G3 will take all reasonable measures to remedy the effects of the data breach and assist Client in mitigating effects of said breach as necessary.

Transfer of Personal Data

G3 will not transfer personal data to, or process said data with, sub-processors which do not provide adequate protection of personal data without informing the Client, unless it does so in compliance with the requirements for the protection of personal data.

Deletion or Return of Personal Data.

Upon expiration of any in-force Service Agreement, or at the termination of each calendar quarter, whichever occurs first, G3 will, at the request of the Client, return or delete personal data, unless there is a legal requirement to store said personal data under government law to which the G3 is subject.

Staff Training

In order to ensure compliance with data protection provisions of in relation to the protection of personal data, G3 will raise awareness and implement training of staff involved in processing operations.

Dedicated Data Center Infrastructure

G3 uses a highly secure data center infrastructure. The hardware and software in each data center is 100% owned, operated, and managed by G3's IT team. True 100% isolation of the data services eliminates the possibility any service interruption, performance degradation, or malware infection that might otherwise be caused by adjacent applications. Combined with multi-level redundancy, the data services infrastructure represents one of the most secure, reliable, and available cloud service architectures available on the market.

- Co-location model with hardware and connectivity 100% owned, operated and managed by G3's IT G3
- Tier 3, SSAE-16 Audited, 24x7x365 staffed data centers with 99.999% uptime, layered security, and biometric access control
- ICSA-certified firewalls
- Clustered server farms for service load-balancing, scalability, and failover protection

Testing, Risk Assessment, and Compliance

The data centers utilized are audited against AICPA SSAE-16 criteria for system availability and security, thus providing assurances regarding adequate oversight over the controls utilized in the processing of information.

The data service center's multi-faceted approach to testing and risk assessment incorporates periodic third party penetration testing of Web, Agent, Firewall, Operating System, Directory Services, and APIs.

Backup and Disaster Recovery Protection

All G3 systems and client data within the data service center are backed up daily to multiple redundant systems in geographically separated, secure locations. G3's shared file directories are backed up to both on-premise and remote, secure datacenters on a nightly basis. All of the G3's virtual desktops (which are assigned to G3 employees) as well as the dedicated servers, are fully cloned using image-level backup procedures, every night, in a separate process from the file share backups, onto dedicated pickup storage systems. All backups are maintained for at least seven days, and are, by design, only accessible by IT team members, not by end-users or their applications. This mitigates the possibility of data being affected by crypto-locker type viruses. Because backups and previous file versions are stored separately and only accessible by administrators through a secure process, they are inaccessible to PC-based viruses, and administrators have the ability to recover damaged content.