Data Privacy and Access Control Policy

Telelink respects the privacy of all individuals and takes very seriously its responsibilities under the Personal Information Protection and Electronic Documents Act (PIPEDA, Canada) 2000, The Health Insurance Portability and Accountability Act (HIPAA, USA) 1996 and The General Data Protection Regulation (GDPR, EU) 2016/679. All data being collected, processed, stored or replicated by Telelink will be managed through the following guidelines.

1. Data Flow (Collected During Processing)

Operators (call takers) receive calls from data subjects through a protected ACD (Automatic Call Distribution) switch. The ACD switch is programmed with queues and distribution groups which direct inbound calls through a multi-tenant, multi-operator ACD environment. Operator accounts are configured with access permissions to reflect a skillset that is assigned to a particular distribution group or access level. Only individuals requiring access to data for the purpose of processing this data has such permissions and skillsets. In some cases an operator would be required to provide live chat or inbound/outbound email services by using a third-party platform that may use cloud services for data processing and storage.

2. Locations of Data (During and After Processing)

- Volume level onsite and offsite backup devices
- File level onsite and offsite backup devices
- DFS for audio recording storage and replication
- In the case of third-party email/chat service, data may be stored in a cloud environment
- Database server
- Telephony switch and supporting applications

3. Protection of Data (Physical and Software)

- Proximity card security system with access schedule
- Security camera system on all sensitive areas
- Fire suppression system in locked server room
- Redundant power utilizing UPS and Diesel Generator
- Redundant file and volume level backup appliances
- Centrally managed anti-virus system for monitoring and deployment of updates
- Redundant firewalls with strict access rules, port management and gateway anti-virus
- LDAP managed permission sets for operators with group based access levels
- Rigorous system maintenance schedule with organized drills and restore cycles
- Data Protection Officer and Privacy team to address data breaches as an ongoing process

4. Access to Data

Volume Level Backup Devices (Onsite/Offsite)
- Direct access to devices is available only to Manager, System Administrator, IT Technician

File Level Backup Devices (Onsite/Offsite)
- Direct access to devices is available only to Manager, System Administrator, IT Technician

Database Server
- Direct access to Database Server is available only to Manager, System Administrator
- Data can be accessed for processing through an ACD switch (for call taking)
- Data can be accessed for processing via scripting engine (programming and reporting)

Telephony Switch
- Operators using this switch are able to access information stored in respective accounts
- Some data, such as on call schedules may be stored in the ACD Switch

5. Remote Access to Telelink Systems

On certain projects Telelink will employ the use of remote workers under a strict and secure set of guidelines. All remote connections require an SSL VPN using military grade, AES-256 bit encryption. The remote worker is required to connect through VPN and then to an encrypted RDP (Remote Desktop Protocol) session which is physically secured within Telelink's infrastructure. Remote equipment is assessed for compatibility, security and comfortable user experience at the time of deployment.

6. Data Retention

Information pertaining to messages, custom reports or other file formats that will be collected on behalf and by the direction of a client will be held and protected by Telelink for one Calendar year. Rollover removal of data will be managed on a monthly schedule.

Any explicit request from the Client to restrict processing, delete, modify or make personally identifiable data portable will be treated as an exception to the retention period and will be undertaken as requested by the Client with an associated processing fee as defined in the Service Contract with Telelink.

7. Disclaimers

Email

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please

notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. If you are not the intended recipient, you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.