ClickReach Data Management & Control Policy

Policy for the Control of electronic data for the purposes of business operations to include, but not limited to:

1. Data access controls and security
2. Identity validation
3. Data transportation
4. Data storage
5. Data backup including storage and transportation of backups
6. Data retention policies
7. Data disposal

Overview of Systems:

ClickReach utilise a variety of methods to meet industry best practice for the handling and management of data. This following section provide details of these methods to demonstrate our commitment to industry best practice and a culture of continuous improvement.

ClickReach utilise the specialist application suite from Citrix called ShareFile. The application suite provides a secure framework from which we operate across the supply chain; from the moment it reaches our systems through to the point of data destruction.

Secure Data Transportation

Information is received from a variety of sources. Data can only be introduced into ClickReach's systems by secure methods of access and transportation. We ensure inbound data from portal sites is encrypted during in transportation and storage.

For sources of data that do not meet our stringent security standards, we mandate that suppliers upload the data to our secure portal using encrypted transportation protocols. Emailing of data is not permitted and filtered accordingly.

Email

Email is used at ClickReach to send identity validated customers a secure link to access their data from the ClickReach secure Sharefile repository. Email is subject to ClickReach company policy and emailing of data is strictly forbidden and our systems filter emails of such data accordingly.

Secure Data Storage at Rest

All data at rest resides on encrypted storage. This includes our online storage repositories and end-user computing devices. Data backups also reside on full disk encrypted storage and is encrypted during transportation. Data Backups are subject to ClickReach's 30-day retention policy for Customer data.

Secure Distribution and Data Access Controls

Data is passed to customers using the defined secure methods facilitated by the Sharefile platform. The application allows for secure communication of those client lists (files) with granular permissions controls e.g. view-only permission on screen, without save permission. Once a file is securely shared with an authenticated customer, then the customer can view and download the file securely and take responsibility of the data from that point.

Data Retention and Disposal

All customer data is subject to our 30-day removal and destruction policy. Customers data files are electronically shredded at ClickReach after 30 days, using proprietary software. Data backups are subject to 30-day retention and backups are consolidated to ensure that customer data older than 30 days cannot be recovered.