Data Security and Privacy Policy

Overview

TRG is a data-driven consulting company that provides arts, cultural and entertainment organizations guidance and solutions for patron-based, sustainable income. One of the company's primary businesses is the management and analytics research of patron data collected by its individual organizations and community network clients. Additionally, TRG aggregates this data. After stripping out personally identifying information, TRG implements arts consumption research that it uses to inform its consulting practice and the larger field of arts management.

Recent legislation and attention in the U.S. on data privacy has been focused on the collection of personally identifying information (PII) by businesses and organizations, the right of consumers to share or not share that information, and how PII can be used by third parties.Any personally identifying information contained in data that TRG processes and aggregates was collected by TRG clients. Therefore, TRG's data privacy focus is limited to describing to clients the precautions, systems and protections utilized by the company to bring in and store data, and prevent unauthorized data access; to make transparent the security and privacy services/systems utilized; and to demonstrate company compliance with TRG's own data security and privacy controls. And finally, this policy addresses TRG's approach to data disposal and data breach disclosure.

TRG annually retains legal counsel specializing in data privacy to review this Data Security and Privacy Policy, as well as TRG's internal Data Security Controls. This consistent review helps ensure that TRG and its clients' data security risks are mitigated.

a. Personally Identifying Information

Protecting information that could be used to identify an individual's identity is of primary concern politically, socially and legislatively today. As described above, this information is referred to as *Personally Identifying Information*, or PII.

PII is categorized as either *Non-Sensitive PII* or *Sensitive PII*. *Non-Sensitive PII* makes it possible to identify, contact, or locate a single person. For example, names, addresses, phone numbers and email addresses constitute *Non-Sensitive PII*. When *Non-Sensitive PII* is combined with other information it is possible to construct behavioral profiles of individuals and groups of individuals that can be used for analysis and marketing purposes. This is the category of PII that TRG stores and uses on behalf of clients.

Personally Identifying Information, continued
Sensitive PII is currently defined by the Federal Communications Commission (FCC) as credit card numbers, financial account numbers, government issued ID numbers, health information, or information regarding children. Both federal and state-by-state laws exist to regulate the collection and storage of this information. TRG does not store any *Sensitive PII* .

The objective of TRG's Data Security and Privacy controls are intended to mitigate against the risk of a data breach that could result in PII being stolen and used for unauthorized purposes.

b. Data Collection

The data collected by TRG client organizations includes non-sensitive PII, such as names and addresses, as well as purchase transaction information including tickets, subscriptions, donations, memberships and more. The majority of this information is collected and immediately stored in a ticketing or development system owned or leased by the client. It is the responsibility of the collecting organization to govern end user privacy and security processes, based on applicable federal and state laws.

Note that while not all states require privacy policies, the FTC has determined that if an organization has a privacy policy or otherwise makes representations to consumers related to the treatment of consumer data, that policy or representation must be followed. If it is not, the behavior constitutes an unfair business practice.

Related to the subject of data collection is the transportation or transmission of collected data. TRG requires client organizations to utilize its secure data transmission process to protect against the risk of data theft during the file transport process. This method eliminates the need for the common, unsecure practice of attaching data files to emails for transmission.

Clients send data to TRG via SFTP (Secure File Transfer Protocol). SFTP is based on SSH (Secure Shell), which is a network protocol that allows data to be exchanged using a secure channel between two networked devices. TRG also employs a robust firewall to protect data and software assets.

TRG participates in Google's Remarketing online marketing program to present online advertisements to TRG web site visitors who visit other, non-TRG web sites. Google's Remarketing is a feature that enables TRG to reach people who have previously visited our website. Ads can be shown to these customers when they visit other websites in the Google Display Network or when they search on Google using TRG's keywords. The advertisements provide visitors information about TRG promotions. TRG's implementation does not collect any personally identifying information, just the basic IP address information used to identify visitors from TRG. No sensitive PII is collected or used in this process. Google utilizes cookies to collect and store IP and visit information. You may opt-out of Googles use of cookies by clicking here.

c. Data Storage

Data stored on computer storage devices is subject to a variety of data security risks. These include unauthorized access to the actual computers and the physical data center where the computers are located, as well as safe handling of data backup media.

Data Center Security
TRG provides a physically secure data center where the computers, network equipment, source software and data storage media are located. Best practice security controls are utilized to ensure that only authorized individuals have access, all access is logged and access to the data center is recorded with video surveillance, 7 x 24 daily. The data center room itself is located within a building that employs 7 x 24 security personnel, card key access, and multiple secure locking access points.

Data Center Security, continued
TRG also follows a secure data backup process to protect against unauthorized access to backup media and to ensure rapid recovery of client data in the case of multiple types of data loss or corruption. TRG's backup and recovery processes mitigate against risk of natural disasters including fire, earthquake, power loss, and floods. Other data storage risks that pertain to our production computer servers include:

- firewall protection
- login authentication
- secure network connections
- anti-virus and malware protection

Traveling Laptop Security
In addition to data storage on TRG computer servers located in its data center, TRG consultants and staff work with client PII and transactional data on PCs and laptops. TRG controls that mitigate the risk of stolen data from these sources include the use of a central file server where all client working files and final deliverables are located, as well as delivering to clients password-protected data files via portal laptops, and removing the files immediately after client delivery.

d. Data Use

Data Processing
TRG processes client data by performing two primary services that enable its use for direct response campaigns and data analysis/research. The first service is name and address correction, often referred to as "data hygiene" or "NCOA (National Change of Address)", which updates patron address information to current postal service standards. This process enables correct unique household identification. Name and address correction is performed by TRG in-house, while a contracted service with a leading data services provider is used for national change of address corrections. TRG's contract with this provider assures this data is not used for any purpose other than the intended processing. When the cleaned data is returned to TRG it is validated for record counts and stored within the secure data center.

TRG also offers clients either self-service or TRG-administered segmentation . This service aggregates patron data into manageable segments, making list creation, trades, and reports much simpler to work with.

Access to Personal Data
TRG provides safeguards to protect data that is accessed directly by clients.

Following periodic processing updates, data is made available to client organizations using powerful self-service web-based tools for List Building, List Trading, Reporting and Analysis. Built into these tools are auditing services that enable TRG to track activities performed by authorized users. Audit records can be used to investigate suspicious application-level activities.

As described in the Overview, TRG retains rights to utilize aggregated data, which is stripped of PII. The aggregation process itself ensures that the risk of disclosing PII is removed.

e. Data Disposal

TRG will honor client requests to remove from its data center PII and transaction data provided to TRG for data services. The process utilized by TRG removes names, addresses and the associations to transaction and organizational information. This enables TRG to retain aggregated data for trend analysis while removing all data specifically related to an organization's patrons.

TRG's process includes data removal from the following sources:

- TRG databases that contain patron files. These currently include both eMerge and new Data Center databases.
- Data on database backup disks are cycled every 30 days, eliminating all previously backed up data.
- Client data product files. These may include working files, final analytics products, and presentations that include data.
- On or around desks of analysts and consultants assigned to the client project. Note that TRG policy forbids the retention of paper output that includes client data. In some circumstances working reports are printed for internal meetings, which are identified and disposed of using a shredder.
- Consultant PC's used for delivering client presentations are reviewed for any stored client presentations or reports, which are destroyed

Data disposal projects produce a final report that records the activities taken for the removal of each source listed above. This report is shared with the requesting organization and retained for TRGs records.
TRG's Data Disposal service requires a request in writing from the primary contact at the client or partner organization. Thirty days are needed to complete a full data disposal project.

f. Data Breach Disclosure

Security breach is defined as an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PII maintained by an entity. In most US states statutes are in place that requires notification to consumers when an entity becomes aware of a data security breach.

If a TRG security breach was to occur TRG would immediately notify the affected organizations, provide a complete list of all patrons believed to have been compromised, and would work closely with organizations to satisfy notification obligations.

This concludes TRG’s Data Security and Privacy Policy.