Data Protection Standards - Samuel Hall

Purpose

This Data Protection Policy (DPP) defines the principles and standards developed and implemented by Samuel Hall for the processing of data and personally identifiable information. Samuel Hall ensures compliance with the strictest data protection standards for its services by implementing the criteria listed below through its standard operating procedures, processes, and technologies.

Terminologies

Any information belonging to a recognized or identifiable individual is considered personal data (PII). An identifiable individual is one who may be recognized through reasonable means, either directly or indirectly, by referencing an attribute or a combination of attributes within the data or combining the data with other relevant information.

Introduction

Samuel Hall's primary and secondary data collection activities require that information about people be collected and used. Respondents to primary data collection can include research subjects, clients, program beneficiaries, and other stakeholders with whom the organization has a relationship or may need to communicate.

The Data Protection Policy was designed to highlight Samuel Hall's rules and regulations for collecting, handling, and storing data, as well as Samuel Hall's transparent commitment to local laws and globally recognized safeguarding and data protection standards. Furthermore, the Data Protection Policy seeks to safeguard the rights of employees, research subjects, partners, and the organization in the event of a data breach.

Data Sharing Agreements

Formal agreements between data sharing parties outline the terms and conditions of the data sharing process. These agreements define the purpose, scope, duration, and responsibilities of each party involved. They also establish legal and contractual obligations to protect shared data and ensure compliance with data protection regulations.

Data Protection Regulations

The General Data Protection Regulation specifies how organizations, including Samuel Hall, must collect, handle, and store personal information, whether it is collected electronically and stored on a computer or as hard copies stored in a filing system. Personal information must be collected and utilized fairly, preserved securely, and not revealed unlawfully to comply with the law.

We respect eight key principles, which state that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Samuel Hall also abides by the laws and regulations of the communities in which it operates.

People, risks, and obligations

Policy Scope

Quarterly or on a case-by-case basis, Samuel Hall reviews and updates its data protection policy. Wherever personally identifiable information is collected, the rationale is disclosed in a transparent manner, either through formal IRB or ERB approvals or contractual agreements.

Whom this policy applies:

- Every office held by Samuel Hall
- Whoever has a part-time, full-time, intermittent, continuous, or permanent employment relationship with Samuel Hall.
- All independent contractors, consultants, and suppliers operating on behalf of Samuel Hall

Additionally, personally identifiable information is collected with the individual's verbal and/or written consent. In every interaction with an individual that any of the above-mentioned parties have at Samuel Hall, data security and privacy are explained and maintained.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Other information concerning individuals.

Privacy Policy

Data Security Threats

Samuel Hall is committed to maintaining open lines of communication with all of its clients and partners. All relevant representatives will be notified in the event of a data breach. This policy protects Samuel Hall from some very real data security threats, such as:

- Violations of confidentiality. For example, information is being disseminated in an ineffective manner.
- Failure to provide options. For example, everyone should be able to choose how their personal data is used by the organization.
- Reputational harm. For example, if hackers successfully gained access to sensitive data, the organization could suffer.

Responsibilities

Everyone who works for or with Samuel Hall is accountable for ensuring that data is collected, stored, and handled correctly and in accordance with applicable laws.

Each team that handles personal data must ensure that it is handled and processed in accordance with this policy and the principles of data protection.

These individuals, however, have important responsibilities:

- Samuel Hall's legal obligations are ultimately the responsibility of the board of directors.
- The research team oversees:
    - Keeping the executive team informed of data protection responsibilities, risks, and issues.
    - Following an agreed-upon schedule, reviewing all data protection procedures and policies.
    - Organizing data security training and advice for those covered by this policy.
    - Answering data protection questions from employees and others covered by this policy.
    - Managing requests from individuals to view the data Samuel Hall has on file for them (also known as 'subject access requests').
    - Examining any contracts or agreements with third parties who may have access to sensitive company data.
- The data protection officer is responsible for
    - Ensuring that all data storage systems, services, and equipment meet acceptable security standards.
    - Conducting regular checks and scans to ensure that security hardware and software are in good working order.
    - Evaluating any third-party services that the company may use to store or process data. Cloud computing services, for example.

General Staff Policies and Procedures

The only people who should be able to access the data covered by this policy are those who require it for their jobs.

- Informal data sharing is not recommended. Employees can request confidential information from their line managers if they need it.
- Samuel Hall provides ongoing training to all employees to help them understand their responsibilities when dealing with data.
- Employees must take reasonable precautions and follow the guidelines below to keep all data secure.
- Strong passwords must be used, and they must never be shared.
- Personal information should not be disclosed to unauthorized individuals, either internally or externally.
- Data must be reviewed on a regular basis and updated if it is found to be out of date. It must be deleted and disposed of if it is no longer required.
- If employees are unsure about any aspect of data protection, they must contact the relevant person.

Data Storage

When a project requires the collection of personally identifiable information, technical and practical safeguards are put in place to ensure that only the authorized employees or clients have access to the data. In some cases, Samuel Hall's research team is required to access personally identifiable information in order to fulfill formal agreements and purposes. To prevent unauthorized external access to personal data, security measures are implemented, some of which are described below.

These rules specify how and where data should be stored safely. Questions about data storage security should be directed to the IT manager or data controller.

When storing data on paper, it should be kept in a secure location where unauthorized people cannot access it.

These guidelines also apply to data that is typically stored electronically but has been printed for a variety of reasons:

- When not in use, papers and files must be stored in a locked drawer or filing cabinet.
- Employees must ensure that no paper or printouts are left where unauthorized people can see them, such as on a printer.
- When data printouts are no longer needed, they must be securely disposed of.
- Data stored electronically must be safeguarded against unauthorized access, accidental deletion, and malicious hacking attempts.
- Data must be safeguarded by strong passwords that are changed on a regular basis and are never shared among employees.
- If data is stored on removable media (such as a CD or USB), these must be securely stored when not in use.
- Data must only be stored on designated drives and servers and uploaded to a cloud computing service that has been approved.
- Data should be backed up on a regular basis. These backups must be tested on a regular basis, according to the company's standard backup procedures.
- Data should never be saved to laptops or other mobile devices such as tablets or smart phones.
- All servers and computers that store data must have a firewall and approved security software.
- Data Access Logs and Audit Trails: Implementing comprehensive logging and auditing mechanisms allows tracking and monitoring of data access activities. This helps identify any unauthorized access attempts, trace the history of data access, and facilitate accountability in case of data breaches or incidents.

Data Use

Samuel Hall adheres to the data minimization principle, data minimization refers to sharing only the necessary and relevant data, reducing the risk associated with exposing excessive information. Before sharing data, a careful assessment should be conducted to determine the minimum required data elements needed to achieve the intended purpose. Following the completion of a specific data collection activity, Samuel Hall ensures that all unnecessary data is properly deleted in accordance with data protection standard operating procedures.

Samuel Hall does not value personal data unless it is required or provided by clients under a formal contractual agreement. However, when personal data is accessed and used, it is most vulnerable to loss, corruption, or theft.

- When working with personal data, employees must ensure that their computers' screens are always locked when unattended.
- Personal information should not be shared informally. It should never be sent via email, as this method of communication is not secure.
- Before data can be transferred electronically, it must be encrypted. SH's data point of contact can explain how to send data to authorized external parties. Encryption is a technique used to transform data into an unreadable format during transmission. This ensures that even if unauthorized individuals intercept the data, they cannot understand or misuse it.
- Employees are not permitted to save copies of personal data on their own computers. Always use the central copy of any data to access and update it.
- Access Control and Authentication: Access control mechanisms are implemented to restrict data access to authorized individuals.

- Data Masking/Anonymization: Before sharing data with other team members, sensitive or personally identifiable information (PII) can be masked or anonymized to protect the privacy of individuals. This involves replacing or removing identifiable information while preserving the data's statistical or analytical value. Techniques such as data perturbation, generalization, or tokenization can be used to achieve this.

Subject Access Requests

All individuals whose personal data is held by Samuel Hall have the following rights:

- Ask what information the organization holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the organization is meeting its data protection obligations.
- A subject access request is made when an individual contacts the company and requests this information.

Individuals should submit subject access requests to the data protection officer via email at info@SamuelHall.org. Before providing any information, the data protection officer will always verify the identity of anyone making a subject access request.

Other Reasons for Data Disclosure

Under certain conditions, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the data subject's consent.

Under these conditions, Samuel Hall will disclose requested data in accordance with the law and signed agreements with clients. The data controller will also ensure that the request is legitimate, enlisting the assistance of senior management and the company's legal counsel as needed.

Providing Information

Samuel Hall's goal is to make sure that people are aware that their data is being processed, that they understand how the data is being used, and that they know how to exercise their rights. This is commonly conveyed during the consent process.

Data Incident Response Plan

A well-defined incident response plan should be established to address any data breaches, incidents, or unauthorized access. This plan outlines the steps to be taken in the event of a security breach, including containment, investigation, notification, and mitigation of potential risks.

Ensuring Data Timely Disposal

Shared data should only be retained for as long as necessary to fulfill the purpose for which it was shared. Clear policies and procedures should be in place to ensure proper data retention and disposal, either by securely deleting data or by anonymizing it in accordance with applicable data protection regulations.

- Data must be kept for as little period as feasible. That timeframe should consider the reasons why your firm or organization must handle the data, as well as any legal responsibilities to store

the data for a specific amount of time. In addition, the organization must guarantee that the data it maintains is correct and up to date.

- According to Art. 17 in GDPR, all respondents have the right to be forgotten.
- To reinforce the right to be forgotten online, the right to erasure should be expanded such that a controller who has made personal data public must instruct controllers processing such personal data to erase all links to, copies of, or replications of those personal data. This processor should take reasonable efforts, considering available technology and means, including technical measures, to inform controllers processing the personal data of the data subject's request. (Check this resource)
- Simply moving files to the "recycle bin" and emptying the bin is not sufficient to thoroughly erase sensitive data. There are several software options for removing all files.