Global Data Privacy Policy

Revision History

Version	Date	Author	Reviewer	Summary
1.0	August 2023	Marie Simonelli	John Livingston, Bill Morrison, Imtiaz Kiyani, Global Privacy Committee Members	New

Table of Contents

Overview

Samsonite International S.A. and its subsidiaries ("Samsonite") process several categories of data belonging to and about its customers, employees and their dependents, vendors, and others to conduct its business processes. Samsonite strives to protect the data it processes to comply with various regional and jurisdictional regulations and requirements and reduce the risk of harm to individuals and the company itself.

Purpose

The purpose of this Policy is to inform Samsonite employees of their obligations related to handling of data; particularly sensitive and/or personal data. Employees should consult with their regional Legal or Data Privacy colleagues with any questions or seek guidance regarding handling, collecting, or processing sensitive and/or personal data.

The Samsonite Data Privacy Office administers this document. It will be reviewed annually, or when material business changes occur, to ensure it remains up to date. Any questions should be directed to Privacy@Samsonite.com.

Scope

This Policy applies to all Samsonite employees globally. Employees should read the Policy in its entirety.

For purposes of this Policy, the term 'employees' refers to permanent and temporary staff, contractors, interns, and any other individual acting in an employment capacity for any Samsonite brand or company.

The data handling requirements outlined in this Policy apply to data in all formats, including electronic and hard copies (paper).

Roles and Responsibilities

Data is an asset to our business operations and appropriate care must be taken by all employees, as they are the first lines of defense against unauthorized or improper use or access. All individuals with access to data, particularly personal, sensitive, or confidential data, are expected to comply with this Policy and seek appropriate guidance to address any questions or concerns.

The Samsonite Data Privacy Program may be administered by Privacy Analysts, Managers, and Directors whose responsibility is to carry out the program's day-to-day activities. These activities include, but are not limited to:

- Responding to Data Subject Rights Requests and other privacy inquiries from external sources.
- Conducting data mapping and data inventory activities.
- Providing Privacy training and guidance to employees and enhancing awareness of the program.
- Developing, implementing, documenting, and maintaining various privacy-related processes to ensure compliance with applicable regulations and data protection best practices.
- Collaborating with business units and corporate functions to address privacy-related requirements and respond to questions and other requests for assistance in Privacy-related matters as needed.

Several employees from various business units may also act as local or regional 'Privacy Champions' to assist with questions about business processes, carry out communication activities, and be a point of contact and reference for privacy-related matters in their jurisdiction.

A Global Data Privacy Committee with representation from each global region meets quarterly to discuss various Privacy-related topics and issues and ways to develop and enhance the program.

The Senior Director of Information Security and Privacy and the Chief Information Officer oversee the Samsonite Data Privacy Program.

General Data Privacy Principles & Program Elements

Confidentiality

- Employees with access to personal data, regardless of to whom it belongs or relates to, shall hold the data in the strictest of confidence.
- Personal data must not be shared with anyone unless absolutely necessary, including coworkers.
- Employees who use instant messaging/social media messaging tools should refrain from sharing any personal data, including that of customers or employees, via these applications unless necessary for resolving a customer's inquiry or with proper consent from the individual.

Purpose Limitation

- Personal data must only be used for the purpose it was collected. For example, if personal data was collected for employment purposes, it may not be used for marketing purposes and vice versa.
- Suppose there is a need to use personal data for any additional processing activities. In that case, the data subject must be notified, and in some cases, consent from the data subject may be required.

Data Minimization

- The collection and processing of personal data should be limited to only what is necessary and relevant. If certain data is not necessary to accomplish a purpose, do not collect it.

- Personal data should only be retained for as long as it is needed to accomplish the business purpose. It should not be kept longer than necessary, except in the case of legal or regulatory requirements.

Notice and Consent

- Depending on the data types and the purpose of processing, Samsonite may be required by regulation to provide advance notice to the data subject and/or obtain consent in order to process personal data.
- Any new or additional processing activities involving personal data should be reviewed by Legal or the Samsonite Privacy Office to determine if notice and/or consent is required.

Access to Personal Data

- Access to personal data should only be provided on a need-to-know basis and to those with a legitimate need to access the data, even with Samsonite colleagues.
- Should an employee discover that they have unnecessary access to personal data and/or has mistakenly received personal data, he or she should notify their manager as soon as possible so access may be revoked and/or the data can be permanently deleted.
- System owners should review their systems periodically to ensure access to personal data is limited to those roles and/or individuals needing to know, and remove access deemed unnecessary.

Training

- Mandatory Data Privacy and/or Information Security training will be provided to employees periodically by Samsonite.
- Training may be provided on a general or regional basis, or focused on a particular business area
- Employees shall be required to attend when requested.

Data Subject Rights and Requests

- Data subjects have certain rights based on applicable laws and in certain circumstances. Typically, these rights include:
    - **Right to Know** if their personal data is being processed.
    - **Right to Access** personal data being processed.
    - **Right to Correct** their personal data.
    - **Right to Delete** their personal data.
    - **Right to Opt-Out of Sale or Sharing** of their data.
    - **Right to Receive** a copy of the data being processed.
    - **Right to Object** to personal data collection or processing.
    - **Right to Restrict** the use of personal data.
    - **Right to Unsubscribe** to marketing or promotional communications.

- Employees who are asked to provide corresponding information in response to a Data Subject Requests shall do so as requested in a timely and complete manner within the relevant statutory timeframe as required by law.
- With the exception of trained Customer Experience staff, employees who receive a request from a data subject shall immediately forward the request to the appropriate regional Privacy team listed below. The exception is in the EU, where ALL requests must be forwarded to the EU Privacy mailbox.
    - APAC & Middle East: privacy.asia@samsonite.com
    - EU: privacy@aboutbags.com
    - North America: privacy@samsonite.com
    - LATAM: privacy.latam@samsonite.com

Cross Border Data Transfers

- Cross-border data transfers involve transmitting personal data from one jurisdiction to another or enabling access to or viewing personal data stored in one jurisdiction from another.
- Various regulations impose strict requirements on cross-border data transfers.
- Employees who wish to transmit, access, collect, or otherwise process personal data across jurisdictional borders must contact their regional Legal or Data Privacy team for guidance and approval prior to transmitting any personal data.

Information Security

- Samsonite is committed to protecting the security of the data it processes as well as its information systems. Samsonite implements various security administrative, technical, and physical safeguards in order to protect the confidentiality, integrity, and availability of information.
- Employees shall avoid any practice that may compromise information security and must adhere to established information security practices.
- Employees may receive periodic Information Security training and/or awareness activities (i.e., random phishing tests), and shall complete the requested activities within the required timeframe.
- Questions relative to Samsonite's Information Security program should be directed to information.security@samsonite.com.

Privacy Notices

- Samsonite posts public-facing Privacy Notices on all its websites for consumer-related data, and in some regions, internal notices for employee-related data practices that address the collection, usage, and other processing activities of personal data. These notices may be modified from time to time.
- Many regulations require certain elements be included in our Privacy Notices. Generally, the Notice describes:

  - Types of data collected and processed.
  - The purpose of collecting and processing the data.
  - How, if, and why data is shared, disclosed, or sold to third parties.
  - Data subject rights, choices, and access.
  - Contact information for Privacy related matters.
- Privacy Notices are reviewed and updated annually, or when there is a material change in practice or as required by regulation.

Data Protection Impact Assessments

- Many applicable laws and regulations require businesses to complete and maintain Data Protection Impact Assessments to identify risks arising from processing personal data and develop ways to mitigate that risk.
- Samsonite employees who are asked to provide information about relevant systems and processes shall respond in a timely, factual, and complete manner.

Corporate Asset Usage

- Any electronic or computing devices and associated equipment provided to employees remain the property of Samsonite. Employees should have no expectation of privacy when using any company-owned devices, systems, networks, or electronic or messaging systems.
- Any activity or messages generated while using a Samsonite-owned device, network, or other electronic or messaging system is considered Samsonite property and is subject to discovery. This also applies to backup data.
- Employees are responsible for the security and safety of devices issued to them by the company, and for any personal data contained on the device. Any type of loss, theft, or damage to company-owned devices shall be reported to IT as soon as discovered. This applies both on and off company premises.
- Employees must return all company devices and equipment when employment with Samsonite concludes or when no longer needed during employment.
- Employees should only use personal devices to access company personal data when necessary and must not store or save any company personal data locally on their device.
- Questions regarding the use of corporate assets should be directed to the appropriate regional IT team.

Data Privacy Incidents

- Employees who become aware of an actual or potential Data Privacy incident involving the loss of, or unauthorized access to, personal data shall immediately notify their local Legal and Privacy teams (see page 7 for Privacy team contact information) to provide as much information about the incident as possible.
- Examples of Data Privacy incidents include, but are not limited to:
    - Sending an email containing personal data to the wrong recipient.
    - Attaching the wrong file containing personal data to an email.
    - Lost or stolen devices containing personal data.
    - Lost or stolen paper files or documents containing personal data.
    - Sharing of personal data inappropriately.
    - Any other incident involving the loss, use or acquisition of, or unauthorized access to, personal data.
- Incidents involving Information Security or technology-related matters, such as malware, ransomware, or phishing attacks, should be reported immediately to the appropriate local IT Help Desk.

Data Storage, Retention, and Disposal

- Employees shall store personal data in a secure fashion and shall not leave mobile devices unattended.
- Employees shall maintain a “Clean Desk” practice by not leaving hard copy personal data out in the open. Employees shall store hard copy personal data in locked drawers or filing cabinets.
- Personal data should only be retained as long as necessary to accomplish the intended business purpose, as required by regulations, or as directed by Legal.
- Personal data must be disposed of securely. Hard copy sensitive data must be shredded or destroyed so that it may no longer be restored. Employees shall consult with IT for guidance on the disposal and/or destruction of hard copy data or the deletion of data on electronic devices.
- Employees should retrieve printed documents containing personal data as soon as possible from printers and printer areas.
- Employees should avoid storing personal data on USB sticks or thumb drives. If use of such devices is necessary, they must be encrypted. Employees should consult with local IT for guidance.
- Files containing personal data should be password protected where feasible. Consult with local IT teams for assistance where needed.

Third Parties

- There are many requirements that need to be met when contracting with third parties who will be processing personal data on behalf of Samsonite. Many of these requirements are regulatory in nature, and many are put in place by Samsonite to protect the company from loss or damage.
- Contracts with third parties processing personal data on behalf of Samsonite must include an appropriate Data Protection Addendum as provided by and/or agreed to by the Samsonite Legal Department.
- Employees who plan to engage with a third party who will process personal data shall consult with their regional Legal contact prior to entering into a contract with or providing any personal data to a third party.

Appendix A – Definitions

NOTE: For purposes of this policy, the terms 'data' and 'information' (i.e., 'personal data' and 'personal information') are used synonymously, although applicable laws and regulations may utilize one or the other.

- **Confidential Data/Confidential Information:** Confidential information or material that is not generally available to the public and that is generated, collected, or used by the Company, relating to its business plans and strategies, financial data, research, manufacturing and development activities, technology, security measures (including, but not limited to, the Company's controls to safeguard its information and premises), and internal operations. This includes customer and third-party information marked as confidential or that is otherwise known to be confidential.
- **Cross Border Data Transfer:** The transmission of personal data from one jurisdiction to another or enabling access to or viewing of personal data stored in one jurisdiction from another. Many jurisdictions place significant restrictions on such transfers.
- **Data Element:** A single item of data that may identify an individual. Examples include name, address, date of birth, physical characteristics, financial account number, specific location data, etc.
- **Data Privacy Incident:** Any loss or unauthorized access, acquisition or use of Personal Data maintained by the Company or its subsidiaries, affiliates, or partners, including service providers.
- **Data Subject:** An identified or identifiable natural person; the person to whom data relates.
- **Data Classification/Information Classification:** The method of identifying categories of data or information determines the handling requirements for certain data types. At Samsonite, the following Information Classifications are used for categorizing sensitive or non-public data: Confidential Information, Internal Information, Personal Information, and Special Personal Information.
- **Internal Data/Internal Information:** Any information regarding the Company's business activities that is not available to the public, but which does not qualify as Confidential or Personal Information.
- **Personal Data/Personal Information:** Any information that identifies an individual or relates to an identifiable individual, including, for example, an individual's name, contact information, email address, government identification number, passport number, salary, and professional background.
- **Processing:** Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- **Sensitive or Special Personal Data/Sensitive or Special Personal Information (only applicable in some jurisdictions):**
    - A subcategory of Personal Data or Personal Information that carries a higher degree of sensitivity and requires enhanced security precautions and processing requirements.
    - Sensitive categories of data may differ slightly depending on region, but typically include:
        - Racial or ethnic origin

- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health or medical data or history
- Sex life or sexual orientation
- Criminal history
- Government-issued identification numbers, such as SSN
- Taxpayer identification number
- Passport number
- Driver's license number or other government-issued identification number
- Credit or debit card details or financial account number, with or without any code or password that would permit access to the account (including cardholder information)
- Credit history
- Children's personal data
- Precise geolocation data

Applicable regulation should be consulted for exact definitions.