Scout Privacy Statement

Revision History

Version #	Revision Date	Summary of Changes	Updated By	Reviewed By	Approved By
Initial version	1st Aug 2019	Initial version	PwC	John Ambooken	Wolfgang Richter

Contents

1. Scope

The scope of the policy is pertinent to all users/customers who interact with any element of the "Scout Platform" or related analytic services. These interactions include: downloading, installing, teaching and data collection via the Scout Client. Logging in, adjusting settings, managing processes, and gaining insights through the Scout Portal. Interacting with our Analytics team on specific uses cases or data inquiries. These interactions may occur in a production environment, a trial context or any variation of Soroco distributed software.

2. About Scout

Scout is an enterprise application used to measure and improve organizational productivity. Scout provides insights through process discovery that drive the creation of a transformation roadmap. The end point client of Scout is installed on user systems, which continuously tracks user activity on Scouted (approved) applications. The data gathered can be used to highlight exactly what aspects of your business to prioritize with different operational levers (automation, standardization, training, elimination) and what return on investment can be expected.

3. Data collection

a) Scout collects personal data in the following scenario:

- Registration of Admin user
  Personal data collect from admin user:
  - Name
  - Email ID
  - Location
  - Role
- Registration of new user
  Personal data collect from new user:
  - Name
  - Email ID
  - Location
  - Role
- The following pieces of PII may be captured if interacted with Scouted applications. Fields that follow a common pattern will undergo PII scrubbing in attempts to remove them from the database.
  - Email ID
  - IP Address
  - SSN
  - Phone
- Passwords, logins, usernames, and other fields that are obfuscated are not captured by default.

Registration based data is not shared outside of client environment.

b) Scout collects data only from approved applications and URLs. By default, all applications and URLs are treated as Unscouted (unapproved.) Unscouted applications and URLS will only register total time spent by all users from a team collectively.

c) Scout only captures detailed information from scouted applications and URLs, which are pre-approved and configurable. As users work in approved applications as a part of their daily function, Scout captures the interactivity within these applications. Scout collects data such as pages the user visits, where the user clicks within a page, what the user types into input boxes.

d) Only Admin users have access to remove or add any application or URL in the Scouted category through the Scout portal. Users can raise requests to admins to remove or add any applications and URLs from the Scouted category.

4. Data Storage

Scout data resides in two locations: briefly on an end user's computer and eventually in a database residing on the Scout Server. The Scout Server may be cloud-hosted or in a location of the client's choosing.

a) All the data collected by Scout is temporarily stored on an individual's computer before being uploaded to the Scout Server. All the collected data is encrypted (AES256), and after upload removed from the user's local device every 5 minutes.

b) If the individual system cannot reach the Scout Server, for example the computer is not connected to the VPN, the data will be stored locally until the Scout Server is reachable.

c) When leveraging the Chrome extension, data is only stored and processed if the Scout Client is installed and active as well'

5. Data Processing

a) Soroco only process personal data in accordance with the agreements reached with the customer.

b) Customers retain all rights, titles, and interests to their collected data. Soroco acquires no rights to customer data, outside any agreed upon analytic services.

c) Periodic reviews/audits shall be conducted to verify that Soroco team members collect and process personal data in compliance with privacy notices, contracts, and this policy.

6. Data Access

a) Only approved engineers and analysts can directly access the raw data collected by Scout. The following actions can be performed by customer request.

- Delete data
- Edit data (e.g. remove certain info, extract fragments, etc.)
- Create admin-level users

b) Only appropriately privileged users can perform following activities from the Portal:

- Edit Scout user details
- Add manager-level users and end users
- Change team assignments

c) An audit log is generated and maintained for every activity performed above.

7. Incident Management

a) If Soroco becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Soroco (each a "Security Incident"), Soroco will promptly and without undue delay:

- notify the Customer of the Security Incident;
- investigate the Security Incident and provide Customer with detailed information about the Security Incident;
- take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

b) Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Soroco selects, including via email. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

c) Soroco shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

d) Soroco's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Soroco of any fault or liability with respect to the Security Incident.

e) Customer must notify Soroco promptly about any possible misuse of its accounts or authentication credentials or any security incident related to Scout.

f) Scout captures personal information however most of the personal data undergoes PII scrubbing. Any sensitive info, such as passwords, emails, or social security numbers, will automatically be scrubbed from the data. In case any personal data is captured by Scout, the Customer may raise an Incident. Scout team will erase the data per request.

g) For every engagement, one POC (Point of contact) for incident reporting is appointed by the Customer.

h) Should an end user have a concern about the data captured by Scout, the following steps should be followed:
   - End user raises an incident by contacting their POC
   - POC will inform Scout Team
   - Scout Team will erase the data

8. Data retention and disposal

a) The default data retention policy is 60 days on the Scout Server. The expiry date/retention period can be configured according to the customer's requirement.

b) After defined retention period, the data will be deleted from the Scout Server on a first-in-first-out (FIFO) basis.

c) All data collected from Scout will be deleted within 60 days after the end of the engagement, unless otherwise mentioned in the contract with the client or by written request from the client.

d) For Scout's Trial version, the data will be deleted after the expiration or termination of customer's subscription.

9. Opt-out option

a) When not performing business-related work, users can pause Scout from collecting data.

b) To pause Scout on their computer, users may perform the following steps:
   - Navigate to the system tray and access the Scout icon.
   - Right-click the Scout icon
   - Click "Pause Scout" button

10. Data Subject Rights

Soroco will make available to Customer in a manner consistent with Soroco's role as a processor Personal Data of data subjects and the ability to fulfil data subject requests to exercise their rights under the GDPR.

Soroco shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request. If Soroco receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with Scout for which Soroco is a data processor or sub processor, Soroco will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of Scout. Soroco shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities: Soroco shall maintain all records required by Article 30(2) of the GDPR and, to the extent applicable to the processing of Personal Data on behalf of Customer, make them available to Customer upon request.

11. Resolution of Disputes

a) *Resolution of disputes reported by Customers*

Customer with inquiries or complaints about the processing of their personal data shall bring the matter to the attention of the DPO in writing. Any disputes concerning the processing of the personal data will be resolved by the DPO by following due process of law through arbitration.

b) *Monitoring and Enforcement*

For the purpose of periodic monitoring, the following processes shall be implemented:

i. *Compliance Assessments*

The DPO shall work with the risk leadership to develop processes to carry out periodic reviews for all functions and customer operations to ensure processing activities are carried out in line with this policy.

12. Validity

This Policy may be revised at any time. Notice of significant revisions shall be provided to employees through the Intranet Portal of Soroco or e-mail communication and to others through an appropriate mechanism selected by the DPO.

This Policy shall be available to customers through the Scout Portal or via Soroco's central documentation site.

13. For Further Details

For more information, such as your rights in respect of your personal data, transfer of personal data, data retention and security measures implemented by Sirocco, please click here.

In the event of a conflict between this Scout privacy statement and the terms of any agreement(s) between a customer and Soroco for Scout, the terms of those agreement(s) will control.

14. Key Terms & Definitions

Term	Definitions
Data Controller	The entity that determines the purposes, conditions and means of the processing of personal data
Data Subject	A natural living person whose personal data is processed by a controller or processor
Data Processor	The entity that processes data on behalf of the Data Controller
Processing	Any operation performed on personal data, whether or not by automated means, including collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Third Party	Third party, in relation to personal data, means any person other than the data subject, the data controller, or any data processor or other person authorized to process data for the data controller.
Personal Data	Any data related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. e.g., Name, Address, Phone Number, IP Address etc.,
Sensitive Personal Data	Sensitive Personal Data is defined as information that if lost, compromised, or disclosed could potentially harm, cause inconvenience, embarrassment, or unfairness to an individual. e.g., Bank account information, Government ID's, Income or Credit history, Credit/Debit card No, data relating to offenses, or criminal convictions, Sexual Orientation, Health/ Medical records either Past or Present or Future, Racial or ethnic origin, political opinions, religious or philosophical beliefs etc.,
Scouted (approved)	Applications and URLS that have been approved to collect granular data from. The info collected include the pages users visited, fields they clicked, and inputs they typed.
Unscoured (unapproved)	Applications and URLs that have not been approved to collect granular data from. The only info that will be collected from these is the duration of time users spend.