
Forcepoint
Remote Browser Isolation
Management of Personal Data

CONTENTS

Disclaimer

This document contains information regarding Forcepoint products and/or services. The information is Forcepoint's property. While every effort was made to ensure the content is up-to-date and accurate, the information is provided AS IS, without any representation or warranty, express or implied, and is subject to change without notice. Any references to future releases or functionality are forecasts and not intended to be commitments. Forcepoint assumes no liability for the use of this information.

General

Document Purpose

This document is designed to answer the question: "What personal data is stored with Forcepoint Remote Browser Isolation?" It is primarily intended for those involved in the procurement and privacy assessment of Forcepoint Remote Browser Isolation.

Privacy Laws

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) was adopted on April 27, 2016 and came into effect on May 25, 2018. GDPR, along with other applicable data privacy laws, guide the principles that are incorporated in Forcepoint's privacy policies and processes, both internally and externally. Full details of the GDPR can be found in various sources, including https://ec.europa.eu/info/law/law-topic/data-protection/reform_en.

Forcepoint Remote Browser Isolation is designed to comply with applicable data privacy principles, including those contained in GDPR. Consistent with these principles, Forcepoint's customers are considered to be the sole data controller. Forcepoint is the data processor with respect to customer data transferred through or stored in Forcepoint Remote Browser Isolation.

Personal Data

This document adheres to the definition of personal data as defined in article 4.1 of the General Data Protection Regulation, which defines 'personal data' as any information relating to an identified or identifiable natural person ('Data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Safeguarding Personal Data

Forcepoint uses industry-standard techniques to protect data held within the Forcepoint product, including personal data. Full details on Forcepoint's privacy policy and processes can be found at: https://www.forcepoint.com/forcepoint-privacy-hub.

User Browsing Data Management Details

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Web traffic redirected from Web Gateway	1) Username (Not required for anonymous browsing) 2) Work Email Address (Not required for anonymous browsing) 3) End User IP Address and session ID (To identify user session when troubleshooting) 4) Cookies (Setting available to disable cookies, not relevant for Anonymous browsing) 5) User Browsing History	Using a Zero Trust approach to web access, Forcepoint RBI enables the use of identity-based access control decisions but allows the ability to log web traffic either based on identity or anonymized to fit the different needs of different organizations. In the process to deliver this service it captures below personal data with the following purpose: 1. Username and work email address - Organizations can choose to let the end user browse the internet anonymously or as a named user. For anonymous users, the username and work email address is not captured, however for named users this information is stored for troubleshooting, logging, and mapping browsed sessions to the user. 2. End User IP Address / session ID –	Forcepoint RBI offers an anonymized mode that can be implemented by customers to either prevent the processing of personal data or to remove a username and mask data stored in logs.	Below is the flow for generation, collection, transformation, and storage of data: Step 1: Web traffic that needs to be browsed through remote browser isolation is redirected from the Secure Web Gateway service to Forcepoint RBI. Step 2: Forcepoint RBI validates the Tenant ID before processing the request. Step 3: After validating the Tenant ID, the request is sent to RBC clusters where each user session is isolated in disposable containers. Step 4: In the RBC cluster the web request is fetched, executed, and rendered within a remote browser. The result of this remote rendering is streamed as a pixel stream to the end user. In the process, • Authenticated users – Cookies, IP address, session ID, browsing history, downloaded file and upload file information is captured for reporting, troubleshooting, and logging purposes. • Anonymous users – IP address, session ID, anonymous browsing history (mapped to IP address / session ID), downloaded file and uploaded file information (again mapped to IP address / session ID) is captured for reporting, troubleshooting, and logging purposes.	Cookies - Cookies are stored for the duration of the session and only for signed in users. For anonymous users cookies are not stored. Organizations have the option to enable or disable the storage of cookies at the tenant level. Downloaded and Uploaded Files – Actual files are deleted within 24 hours. User browsing history – Tenant admin has an option to define the data storage duration, based on options of 1 day, 30 days, 60 days, 90 days, 120 days, 150 days, and 180 days. After the data storage duration has been reached all PII information will be automatically anonymized. Additionally, there is an option available for the admin to anonymize the PII information for a specific user upon request.

		This is required to identify end user sessions for debugging and troubleshooting e.g., when a specific user has trouble browsing via RBI and calls into support. This cannot be mapped directly to a specific RBI user without additional external information, such as the user calling into support and sharing their IP address. 3. Cookies - Organizations have an option to enable or disable the storage of cookies. Even when organizations enable the storage of cookie, it will be saved only for signed in users and not for anonymous users. Cookies are required to be stored for providing close to native browsing experience. 4. Session Browsing History- This data is captured for reporting and necessary to determine how policy regulations are working in practice.			

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Currently we are not tagging personal data collected with a PII tag. The customer admin is able to run reports that contain the personal data stored by RBI.
SAR - Correction/Rectification	Forcepoint can manually correct/rectify personal information collected. However, customers cannot correct, rectify, or change information already collected and stored within the stored data logs other than anonymizing the data.
SAR - Right to be Forgotten	Yes. The tenant admin can anonymize data for a specific user. In addition, the data is anonymized automatically after the defined data storage period has been reached. The storage period can be configured by the admin based on their organizational policy.
Data Storage / Localization	Data is stored in cloud data centers and the region can be selected during tenant creation (i.e. US, EU, or APAC). Currently customers cannot choose specific data center regional locations to store data outside of the initial selection during tenant creation.

Tenant Admin Login to RBI Admin Portal

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Admin login to RBI Admin Portal. The email address, first name, and last name of each admin are stored in the database.	The email address and password used to login to the Admin Portal.	Administrators need to login to the RBI Admin Portal to define policy rules, to investigate alerts and threats, and to download any reports for internal use.	We do not pseudonymize/mask the admin data, which consists of systems policies and user account information.	All communications in FP RBI are protected using TLS Certs. Communication between the user browser & FP Admin Portal is via https and only Authenticated admin users can login. RBI database itself is stored on EFS which is encrypted using KMS Key • All files are stored on EFS which is encrypted using KMS Key • All passwords are stored as one way hash.	Admin data is deleted upon deletion of relevant account or if the data is manually deleted by an administrator.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	The customer has the ability to retrieve admin user information within the platform.
SAR - Correction/Rectification	Forcepoint or customer can manually correct/rectify admin information collected.
SAR - Right to be Forgotten	The admin data will be deleted upon request or upon deletion of the relevant account.
Data Storage / Localization	Data is stored in cloud data centers and the region can be selected during tenant creation (i.e. US, EU, or APAC). Currently customers cannot choose specific data center regional locations to store data outside of the initial selection during tenant creation.