Forcepoint ONE Management of Personal Data

Forcepoint

Table of 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.

©2020 Forcepoint. All Rights Reserved.

General

Document Purpose

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

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 ONE 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 ONE.

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 on the Forcepoint Trust Hub at: https://www.forcepoint.com/legal/forcepoint-trust-hub.

DLP Data

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Data (text, files, etc.) sent to the Forcepoint ONE DLP Engine for inspection. The information gathered includes: - Object name - Type (file, email, fields) - Username - User agent - Company ID - DLP pattern matched	Username, which are used to attribute DLP matches to individual users.	The DLP engine allows Forcepoint ONE customers to control the movement of data across their organization and enforce regulatory compliance around such data. When DLP policies are used, they identify the username associated with the user sending the data that matched the DLP pattern to allow security teams to identify the users and resources involved with inappropriate movement of sensitive information.	Not at this time.	Files or text to be sent to the DLP engine are first encrypted with 256-bit encryption then sent to the data plane. Inspection happens in the data plane with relevant information (e.g., object name, type (file, email, fields), username, user agent, company ID, and DLP pattern matched) logged to local encrypted file systems and the original encrypted file is then deleted from the data plane. Relevant information that is logged is only stored temporarily, until it is sent through the pipelines for Proxy, API, and SWG, which are addressed individually in following sections. All information stored and transmitted is protected with 256-bit encryption. Access to this AWS environment is limited to select personnel. Temporary access to the environment may be provided for problem solving on a case-by-case basis with appropriate approvals.	Since DLP logs are only held temporarily before being fed to downstream SWG, Proxy or API pipelines, there is no data retention here. Following sections include relevant data retention for those data flows.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Since DLP logs are fed to downstream SWG, Proxy or API pipelines, any requests shall be handled in accordance with the process described for the relevant section below.
SAR - Correction/Rectification	Since DLP logs are fed to downstream SWG, Proxy or API pipelines, any requests shall be handled in accordance with the process described for the relevant section below.
SAR - Right to be Forgotten	Since DLP logs are fed to downstream SWG, Proxy or API pipelines, any requests shall be handled in accordance with the process described for the relevant section below.
Data Storage / Localization	Since DLP logs are fed to downstream SWG, Proxy or API pipelines, any requests shall be handled in accordance with the process described for the relevant section below.

Proxy Logs

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Data from requests/response headers. The information gathered includes: - Headers - Cookies - Filename - Doc type - Username - User ID - Email subject, CC, BCC	Username is collected. If there is any PII that might be part of an email subject line, that would also be collected as the email subject line is collected.	Users' http requests are collected and analyzed to log user activity on the Forcepoint ONE platform.	Not at this time.	When user requests flow through the data plane the events are scanned and filtered based on the parameters set in the security policies. The http request data for relevant events are logged to a temporary file in an encrypted file system before being sent to further processing/storage. The temporary file is then deleted immediately. The relevant event data passes through a log processing pipeline that is secured with 256-bit encryption until it reaches databases protected by AWS security groups so that only select services we manage can write to them. All backups are stored using 256-bit encryption Access to this AWS environment is limited to select personnel. Temporary access to the environment may be provided for problem solving on a case-by-case basis with appropriate approvals.	Event data is retained for 30-60 days depending on the day of the month.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data access request. Customers can specify a custom private location (generally an S3 bucket) to copy the data to so that they can access and analyze it.
SAR - Correction/Rectification	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data correction request. The Support team will work with our Operations and Engineering team to perform the data correction. The engineering team will need to request access to the environment to perform any changes.
SAR - Right to be Forgotten	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data deletion request. The Support team will work with our Operations and Engineering team to perform the deletion. The engineering team will need to request access to the environment to perform the deletion.
Data Storage / Localization	For our commercial cloud this data is currently stored in the AWS US-West data center that resides in Oregon. For our EU cloud, this data is stored in Frankfurt, Germany.

API-based Scanning for Data at Rest

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Data pulled from API calls to cloud applications protected by Forcepoint ONE CASB. APIs are used by Forcepoint ONE CASB to identify data at rest in cloud applications. The information collected includes: - File/Object name - Type (file, email, field) - Creator (Username) - Last modifier - Shared with - Subject (in case of email)	The API scanning data includes Username and email subjects which could contain PII in the subject line.	API inspection of data at rest in cloud applications allows visibility and control over sensitive information in cloud applications that are protected by Forcepoint ONE security policies.	Not at this time.	The file/data retrieved from cloud applications flows through our DLP engine for inspection and follows the previously mentioned pipeline using 256-bit encryption. The information produced by the API Scanning is as follows: - Summary Logs – These are logs of the current state of the files that have been scanned for a customer across every application for which they have set up scanning. Each record has the following fields: file/object name, type, size, shared with etc. These logs do not include customer personal data. - Audit Event Logs – These are temporary logs that capture any changes or scans for a particular file. This data is also sent to S3 buckets for building aggregations for dashboards. The Audit Event Logs and Summary Logs are protected using security groups so that only select services can write to them. All the data stored in the S3 buckets is encrypted using 256-bit encryption. Access to this AWS environment is limited to select personnel. Temporary access to the environment may be provided for problem solving on a case-by-case basis with appropriate approvals.	The Audit Event Logs are stored for 30-60 days (depending on the day of the month) for querying. The Summary Logs are stored until a customer requests their deletion. This is to provide a historical view of the files scanned (only meta data of the files).

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data access request. Customers can specify a custom private location (generally an S3 bucket) to copy the data to so that they can access and analyze it.
SAR - Correction/Rectification	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data correction request. The Support team will work with our Operations and Engineering team to perform the data correction. The engineering team will need to request access to the environment in order to perform any changes.
SAR - Right to be Forgotten	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data deletion request. The Support team will work with our Operations and Engineering team to perform the deletion. The engineering team will need to request access to the environment to perform the deletion.
Data Storage / Localization	For our commercial cloud this data is currently stored in the AWS US-West data center that resides in Oregon. For our EU cloud, this data is stored in Frankfurt, Germany.

Secure Web Gateway (SWG) Logs

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Data generated by the web proxy. This information includes: - Username - User agent - User email - Device IP address - Transaction ID - Company ID - URL accessed	SWG Logs contain Username, user email and device/user IP address.	The data is produced to report web browsing activity for the purpose of tuning acceptable browsing policies within an organization.	Not at this time.	SWG Logs are collected on the user's file system. They contain information that includes the user logged into device, username, user email, device hostname, device IP, and user agent. This data gets sent to Forcepoint ONE through an https channel (encrypted using TLS 1.2). Primary storage for these logs is Forcepoint ONE AWS S3 buckets. A subset of the data is also pushed to AWS RedShift from where it can be queried and filtered for logs and dashboards. All the stored data is encrypted using 256-bit encryption. Each customer's data is stored in separate S3 directories and AWS RedShift tables. Access to this AWS environment is limited to select personnel. Temporary access to the environment may be provided for problem solving on a case-by-case basis with appropriate approvals.	30-60 days of data (based on day of the month) is loaded into AWS Redshift for querying on the Forcepoint ONE dashboards and reports. This is a sliding window of data. Data beyond 2 months is deleted from AWS Redshift.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data access request. Customers can specify a custom private location (generally an S3 bucket) to copy the data to so that they can access and analyze it.
SAR - Correction/Rectification	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data correction request. The Support team will work with our Operations and Engineering team to perform the data correction. The engineering team will need to request access to the environment in order to perform any changes.
SAR - Right to be Forgotten	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data deletion request. The Support team will work with our Operations and Engineering team to perform the deletion. The engineering team will need to request access to the environment to perform the deletion.
Data Storage / Localization	For our commercial cloud this data is currently stored in the AWS US-West data center that resides in Oregon. For our EU cloud, this data is stored in Frankfurt, Germany.

Health Logs

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
This data is from Access Logs in the Forcepoint ONE data plane regarding http request/responses. The information gathered includes: - Username - Transaction ID - Company ID - User agent - Response code	The health logs contain Usernames.	The purpose of these Access Logs is to calculate metrics on request and response codes and reporting on any errors in user access.	Not at this time.	This data contains information sent from the data plane to a data analytics cluster. Analytics further summarize the data based on different dimensions, e.g. latency, returned 200s, returned 400s, etc. This data is protected using security groups so that only select services can write to them. Access to this AWS environment is limited to select personnel. Temporary access to the environment may be provided for problem solving on a case-by-case basis with appropriate approvals.	Data is retained in the system for 30-60 days depending on the day of the month.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data access request. Customers can specify a custom private location (generally an S3 bucket) to copy the data to so that they can access and analyze it.
SAR - Correction/Rectification	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data correction request. The Support team will work with our Operations and Engineering team to perform the data correction. The engineering team will need to request access to the environment to perform any changes.
SAR - Right to be Forgotten	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data deletion request. The Support team will work with our Operations and Engineering team to perform the deletion. The engineering team will need to request access to the environment to perform the deletion.
Data Storage / Localization	For our commercial cloud this data is currently stored in the AWS US-West data center that resides in Oregon. For our EU cloud, this data is stored in Frankfurt, Germany.

Shadow IT Discovery Reports Data

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
This data is gathered from the Firewall Logs provided by the customer. There are 2 options: - Directly upload Firewall Log files to the Forcepoint ONE portal; or - Set up log streaming from firewall to Forcepoint ONE. This channel is encrypted using TLS 1.2 using certificates provided by Forcepoint ONE. Firewall Logs are processed based on mappings set by the customer to produce aggregations such as the following: - Top source IPs - Top destination IPs - Volume of data going to and from each source	This discovery data would contain source IP addresses. There is no way to tie this information with the actual Username or User ID directly using the Shadow IT Discovery Logs. The Shadow IT Discovery Logs provide a correlation of the Source IP to the visited Destination IP address.	The Discovery Reports are based on mapping set by the customer to determine the following: top source IPs, top destination IPs, and the volume of data going to and from each source.	No pseudonymization is performed. There is no IP address to Username mapping through Shadow IT Discovery, hence no pseudonymization is possible.	Once the Firewall Logs reach Forcepoint ONE, they are stored for a period (generally a few hours) in an encrypted file system before processing. This file system is encrypted using 256-bit encryption. The data is processed internally and protected using security groups so that only select services can write to them. Access to this AWS environment is limited to select personnel. Temporary access to the environment may be provided for problem solving on a case-by-case basis with appropriate approvals.	The retention period differs based on mode of the upload of the Firewall Logs. - Aggregations from the manual Firewall Logs upload are retained in the form of a Discovery Report within the Forcepoint ONE portal until the customer requests its deletion. - Aggregations from the Firewall Logs streamed to Forcepoint ONE are stored for 90 days. The report in the Forcepoint ONE portal is based on a sliding 90-day window of data. Once data goes beyond the 90 days, it is deleted.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data access request. Customers can specify a custom private location (generally an S3 bucket) to copy the data to so that they can access and analyze it.
SAR - Correction/Rectification	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data correction request. The Support team will work with our Operations and Engineering team to perform the data correction. The engineering team will need to request access to the environment in order to perform any changes.
SAR - Right to be Forgotten	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data deletion request. The Support team will work with our Operations and Engineering team to perform the deletion. The engineering team will need to request access to the environment to perform the deletion.
Data Storage / Localization	For our commercial cloud this data is currently stored in the AWS US-West data center that resides in Oregon. For our EU cloud, this data is stored in Frankfurt, Germany.

Forcepoint ONE AppDB

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Firewall Logs that are being accessed from the Discovery Pipeline, including destination IP addresses of applications being accessed.	There is no personal data collected. It is only the destination IPs of the applications.	The purpose of this is to determine if Forcepoint ONE has the relevant hosts listed in the current AppDB and whether they are connected to an existing application. If not, then the AppDB works out which application the destination IPs belong to and if there are valid SSL certifications for the domains.	No pseudonymization of data, as no personal data is collected.	The destination IPs are put into S3, from where AppDB processes those IPs and converts them into hostnames. Then it performs a match to see if those hosts are in the current AppDB. If not, further work is performed to check which application the destination IPs belong to. All this data is retrieved from public sources.	The data is stored in AppDB but all the data is publicly available information, so it is retained as long as the service is active.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Not required – given the nature of the AppDB data, there is no personal data stored.
SAR - Correction/Rectification	Not required – given the nature of the AppDB data, there is no personal data stored.
SAR - Right to be Forgotten	Not required – given the nature of the AppDB data, there is no personal data stored.
Data Storage / Localization	For our commercial cloud this data is currently stored in AWS US-West datacenter that resides in Oregon. For our EU cloud, this data is stored in Frankfurt, Germany. Not required – given the nature of the AppDB data, there is no personal data stored.

User and Policy Configuration in Config DB

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
This consists of the properties used to configure security and access policies in Forcepoint ONE. The policy conditions includes: - Groups - Access method - Device - Location - Action These include Users and Groups configured, e.g. Username, first name, last name, email address, type, status, and group name.	The details on the users and groups, includes Username, first name, last name, and email address.	These are necessary properties to apply security policies to different users and groups accessing resources that are controlled by Forcepoint ONE.	Not at this time.	Once a policy is saved, it is stored in an AWS RDS database. Also, once a new user/group is synced into the Forcepoint ONE platform or created manually, it is stored in an AWS RDS database. Data at rest within the RDS database is encrypted using the AWS Key Management Service. Access to this database is restricted through AWS security groups so that only select services can write to it.	This data is retained until a customer requests its deletion by deleting the policies, users or groups.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data access request. Customers can specify a custom private location (generally an S3 bucket) to copy the data to so that they can access and analyze it.
SAR - Correction/Rectification	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data correction request. The Support team will work with our Operations and Engineering team to perform the data correction. The engineering team will need to request access to the environment in order to perform any changes.
SAR - Right to be Forgotten	Customers can raise a request on the Forcepoint Customer Hub (support.forcepoint.com) to initiate a data deletion request. The Support team will work with our Operations and Engineering team to perform the deletion. The engineering team will need to request access to the environment to perform the deletion.
Data Storage / Localization	This data within the AWS RDS database is stored in multiple replicas across 6 different regions to provide low latency access for querying the information from individual proxy nodes.