
Forcepoint
Data Protection Service
Management of Personal Data

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.

General

Document Purpose

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

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 Data Protection Service 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 Data Protection Service

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-trust-hub

DLP Manager push policy to Cloud Object Store Service (OSS)

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Customer policies that contain the DLP rules applied to monitor content by the CASB product.	DLP policy rules are crafted to identify network activities of concern, but customers determine policy content and conceivably could write a rule that includes personal data.	The DPS uses the DLP protection rules to enforce the customer data protection policy on files and content stored in the customer Cloud Repositories such as OneDrive or SharePoint online. CASB is the product that connects and fetches the files and content from the customer Cloud Repositories and passes it over to DPS for inspection.	No pseudo anonymization as DLP policies consists of keywords and common expressions that are unlikely to contain personal data warranting pseudonymization. Moreover, policy content is under customers' control.	*The DLP Policy is created on-premises and uploaded to the Object Store Service (OSS) via a secured HTTPS communication (TLS 1.2). the Object Store Service saves the file into the S3 bucket in the Forcepoint AWS account. The S3 is encrypted at rest with AES 256 encryption.* *The policy file is encrypted at rest by the S3 service (AES256)* *The communication between DLP Manager to OSS is secured (HTTPS TLS 1.2 or above)*	*Though the DLP policy file is retained in the S3 bucket, the customer determines the policies and the policy file content Thus, Deletion of the DLP policy is the responsibility of the customer's DLP Manager administrator. The administrator is expected to delete obsolete policies (we intend to keep the last 10 policies in the Cloud)* *No Deletion of policies in DLP 8.8.1 given the complexities that arise from policy cross references and dependencies. Therefore, whilst deleting a policy file is relatively simple (we intend to keep the last 10) however the deletion of the policy dependency files (which are uploaded to the OSS with the policy itself) is complex as it requires significant computing to determine if an old policy dependency*

					file is in use by one of the latest 10 policy files. *Since the policy file and policy dependency files are NOT containing any personal and private information then DLP 8.8.1 does not handle the deletion of policy files and this functionality was deferred to a later release due to its low priority and business value.*

How to Manage Subject Access Request (SAR)

SAR - Right to Access	No provision to support customer response to data subject access requests. This is consistent with the fact that DLP Policies are unlikely to contain personal information out of the box. Moreover, the customer, not Forcepoint, retains data systems of record that are complete.
SAR - Correction/Rectification	The Customer Admin controls the policies and the system component used for updating those policies. Only the customer is in a position to make corrections.
SAR - Right to be Forgotten	The Customer Admin controls the policies and the system components used for policy editing. Only the customer is in a position to execute the request to be forgotten.
Data Storage / Localization	The DLP Policy of a specific tenant is stored in a S3 folder that is dedicated for the specific tenant Each tenant (a sub-set of the customer organization that is treated as a separated/distinct entity) has his data separated from other tenants (of the same customer or of tenants that belong to other customers). The S3 bucket is in the tenant primary region Each tenant has only one primary region and can choose whether to store the data is AWS EU-central-1 (Frankfurt) and for all other customers the primary region sis US-east-1 (North Virginia). Additional regions may be added if warranted by data volume or customer use patters.

DPS downloading the DLP policy from OSS

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Customer policies that contain the DLP rules applied to monitor content by the CASB product.	DLP policy rules are crafted to identify network activities of concern, but customers determine policy content and conceivably could write a rule that includes personal data.	The DPS uses the DLP protection rules to enforce the customer data protection policy on files and content stored in the customer Cloud Repositories such as OneDrive or SharePoint online. CASB is the product that connects and fetches the files and content from the customer Cloud Repositories and passes it over to DPS for inspection.	No pseudo anonymization. The DLP policy contains rules and keywords and regular expressions intended to detect and protect Personal information. Pseudonymization would defeat the objective of enabling personal data protection.	*The DPS which runs inside a Docker (inside AWS Kubernetes) downloads the DLP policy from the Object Store Service (OSS) and load it its memory.* *Every 5 minutes the DPS calls the OSS to check if a newer policy exists, and if a new policy found DPS will download it and replace the previous one.* *The DLP policy is encrypted at rest in the OSS (the S3 is using AES 256) and loaded into the DPS memory* *DPS use HTTPS (TLS 1.2 or higher) to call the OSS and download the DLP policy file.*	*The DLP policy is kept in DPS until a newer DLP policy is available in the Object Store and then DPS will replace its current DLP policy with the newer one and delete the older version.* DLP Admin cannot call today to delete the DLP policy from the OSS. The policy file is unlikely to have personal/private data

How to Manage Subject Access Request (SAR)

SAR - Right to Access	The DLP Policy does not contain out of the box private or personal information. An admin may add keywords into the policy to detect and protect personal information. The admin manages the content and access to the policies.
SAR - Correction/Rectification	Correcting the DLP policy is done by the customer admin editing the policy file via the DLP Manager console. The Customer Admin controls the policies and to the extent the policies contain personal data the admins make those determinations and has the control necessary to make corrections.
SAR - Right to be Forgotten	The admin through their ability to correct the policies can delete personal data to the extent that it is present in the policy.

Data Storage / Localization	The DLP Policy of a specific tenant is stored in a S3 folder that is dedicated for the specific tenant Each tenant (a sub-set of the customer organization that is treated as a separated/distinct entity) has his data separated from other tenants (of the same customer or of tenants that belong to other customers). The S3 bucket is in the tenant **primary region** Each tenant has only one primary region and can choose whether to store the data in AWS EU-central-1 (Frankfurt) and for all other customers the primary region is US-east-1 (North Virginia)

CASB calling DLP to inspect user activities and files

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
The files retrieved by CASB may include any type of data that customer employees store on OneDrive, SharePoint or any other cloud repository that is accessed by the CASB server	The files that CASB retrieves from the Customer Cloud Repository **may** include personal data	CASB retrieve the files and pass them over to DPS for inspection of the data to ensure files containing protected data are not stored in forbidden Cloud locations and are not shared inside/outside the company with unauthorized users. The DPS enforces the customer DLP policy and replies to CASB with a decision about what to do with the files (keep, quarantine, encrypt) based on the DLP policy rules that the customer admin has defined. CASB then executes the decision and encrypts or moves the files to quarantine locations if needed.	No pseudo anonymization, the file is the original file that was on the customer cloud repository and is analyzed in memory and then discarded.	CASB server retrieve files from customer cloud repositories and sends them over a secured communication channel (HTTPS request, TLS 1.2) to the DPS service. DPS extracts the text from the file and inspects the content to find protected information. Then DPS analyzes the text content against the DLP policy to enforce the corporate data protection policy. DPS returns to CASB server the policy engine decision about what to do with the file – permit the file to be kept in its current location with current permissions, or whether to move the file to a different location (quarantine), encrypt the file or simply change the permissions for whom can access the file. The CASB server will perform the DLP policy decision. Communication between the CASB server and the DPS server is over HTTPS (TLS 1.2 or above) secured links. The inspected file is analyzed in DPS memory, which is only accessible by authorized personnel.	The files that are passed to DPS are not retained on the DPS server; the files are discarded (from memory) after the DPS completes the content inspection. The content inspection takes between 2 to 30 seconds. The DPS server may only be accessed by authorized personnel. The files are immediately deleted from the DPS memory after being analyzed If the file triggers a policy rule, then a copy of the original file will be stored temporarily in the OSS (for about 5 minutes) until the DLP manager downloads the file to the local on-premises storage and deletes it from the OSS.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Not supported since analyzed files are not retained in the DPS.
SAR - Correction/Rectification	Not supported since file content is not retained on the DPS and system of record containing the data is in the customer's cloud repository. There is no means for the tool to modify original file content. hence the customer is responsible for data correction
SAR - Right to be Forgotten	The inspected file is not retained as part of the data inspection process, hence nothing to be forgotten. We will address the right to be forgotten in flow "DPS uploading Incident meta data and Forensics to OSS" and "DLP Manager download Incidents and Forensics from OSS" below that describes the data flow of file saved as a forensic and copied to the DLP Manager on-premises.
Data Storage / Localization	The inspected file is not stored as part of the DPS content analysis process. Note: if the file triggers a DLP incident then the file will be sent to the on-premises DLP manager – see data flow "DPS uploading Incident meta data and Forensics to OSS" and "DLP Manager download Incidents and Forensics from OSS" below for more information

DPS uploading Incident meta data and Forensics to OSS

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
DPS analysis of customer files available in one of the customer's Cloud Repositories (such as OneDrive). If the analysis triggers an incident, the incident metadata (XML) as well as r the file. will be uploaded by DPS into the DPS-OSS	The incident meta-data contains information about the repository, the file and the **user** that performed the operation. The file **may** include any type of data, including personal data. Incident metadata will include the user identifier usually in a form of an email address (john.doe@acme.com)	DPS receives the file from CASB to analyze the file content and evaluates it against the corporate DLP policy as configured by the customer DLP admin. If the file triggers a DLP policy rule then DPS stores the file as forensics into the OSS and also the incident meta-data into OSS to enable and support incident investigation	The forensic file is the original customer file and DLP does not modify the customer original files (for example DLP cannot change a docx, or a pdf or excel) furthermore, DLP does not know which keywords inside the original file contain personal data. The incident XML includes the end-user email address (serves as user identification), this information is not pseudo anonymized as it would break the correlation between users and the incidents they triggered which would defy the main functionality of DLP	If the file triggers a DLP policy rule, then DPS will upload the file to the Object Store Service (OSS) and stores incident meta-data as XML into the OSS. The communication between the DPS server and the OSS is secured HTTPS (TLS 1.2 or higher) The data storage in use by OSS is S3 which keeps the files (forensics and XML) encrypted at rest using AES256. Once DLP Manager downloads the forensics file from OSS (see data flow "DPS uploading Incident meta data and Forensics to OSS" below) the DLP manager encrypts the file with a customer specific key and then stores the encrypted file into the forensics network share on-premises.	The forensic file and incident XML are stored in the Object Store service for a short period of time until the DLP manager (on-premises component) retrieves these files from the OSS (see data flow "DPS uploading Incident meta data and Forensics to OSS" below) and then the DLP manager will delete the forensic file and the Incident meta-data XML from the OSS. DLP manager checks for new files in the OSS every 5 minutes.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	The forensics file and Incident meta-data (XML) are stored for a short period in the Object Store (S3 bucket in the Forcepoint account) Since the data is automatically deleted from the OSS within 5 – 10 min then the subject cannot access the files in the OSS. Note: in data flow DLP Manager download Incidents and Forensics from OSS below that describes the DLP Manager storing the Incident and Forensics, the Subject can request to access the data.
SAR - Correction/Rectification	The data is read only and is immutable. If the data is corrupted it is simply deleted and not repaired. The data must not be modified to server as forensic evidence for the incident. However, the entire incident can be marked by the DLP admin as a false-positive and can be deleted from the on-premises storage (see data flow DLP Manager download Incidents and Forensics below)
SAR - Right to be Forgotten	The files are automatically deleted from the Object Stores Service within 5-10 min once the files are downloaded to the on-premises DLP manager, so the file is automatically "forgotten" Note: the right to be forgotten is applicable in data flow DLP Manager download Incidents and Forensics below after the file is downloaded and stored in the on-premises DLP Manager
Data Storage / Localization	The forensics files and incident meta-data (XML) are stored for short period in an S3 bucket in the DPS production account until they are downloaded to the on-premises DLP manager. All files in the S3 the files are encrypted at rest using AES256

DLP Manager download Incidents and Forensics from OSS

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
The forensic file is any customer file that was on a customer Cloud repository and triggered a DLP policy rule. The Incident meta-data contains info about the file, the cloud application, the storage, and user that performed the DLP policy violation	The forensic file **may** include personal data as it can be any file that any customer employee uploaded to the customer cloud repository. The incident meta-data contains information about the sensitive data found in the forensics, the cloud storage where the file was found and in some cases about the user that uploaded (or shared) the file to the repository	The file contained sensitive information (could be intellectual property or any other type of data that the customer determined to be sensitive) and triggered a customer defined DLP policy rule. Keeping the file as forensics and downloading it as well as downloading the incident meta-data (XML) to the DLP manager on-premises allows the customer DLP admin to investigate the file along with the incident meta-data	The forensic file is the original customer file and DLP does not modify the customer original files (for example DLP cannot change a docx, or a pdf or excel) furthermore, DLP does not know which keywords inside the original file contain personal data. The incident XML includes the end-user email address (serves as user identification), this information is not pseudo anonymized as it would break the correlation between users and the incidents they triggered which would defy the main functionality of DLP	DLP Manager checks every 5 min if forensic files and/or incident files exists in the Object Store Service (OSS). If files (or incident XML files) exist then DLP manager will download these files, store them locally and then delete the files from the OSS. The DLP Manager does not keep records of which files it already downloaded and deleted, instead the DLP manager always check if files exists and if there are files then it will download them (even for a second time) and delete them. This ensures that the OSS will eventually be empty. The SQL database that stores incidents is protected by user/password (it is a Microsoft SQL server). The customer can configure additional encryption settings to the database (the database is owned and installed by the customer, Forcepoint creates tables inside the customer database but does not administer the	Incidents are not retained on the OSS. In the DLP manager SQL database the incidents are kept inside database tables for 3 years and then deleted automatically. There is no configuration today to control the period of data retention. Forensic files not retained on the OSS, once the DLP manager downloads the forensic file it encrypts the file (AES256) and store it encrypted on local drive. There is no scheduled deletion/retention of the forensic files. Incidents can be deleted by the Admin via the UI. Incidents are also deleted after 3 years automatically from the database. Forensic files are deleted when an incident is marked as "closed" by the DLP admin via the console UI (this setting can be turned off).

				database) Forensic files are encrypted by DLP Manager before being stored on a network share (on-premises)	

How to Manage Subject Access Request (SAR)

SAR - Right to Access	The DLP manager SQL database is installed by the customer on the customer premises, and protected by user/password, any customer IT person with possession of the user/password can connect directly to the MS-SQL database. Forensic files are stored encrypted on disk, even if the customer IT person has access to the network share location, he cannot read the content of the encrypted files. Only DLP admin that have access to the DLP Manager user interface can view the forensic file content, as the DLP manager decrypts the forensic file before opening it for the DLP admin.
SAR - Correction/Rectification	The incident content cannot be modified, however the ***customer admin*** can change the severity and the status of an incident, for example set the incident to false-positive or even delete the incident. Other meta-data of the incident cannot be changed (time, user, classifications that were found) Forensic files cannot be modified, they are original customer files that were identified as containing sensitive information and hence triggered the incident. The forensic file can be deleted as result of the incident deletion. The employee details that are included in an incident are the username and manager (which are taken from the active directory) if these details are incorrect then fixing them in the active directory will not fix the details in the incident, but it will fix all future incidents.
SAR - Right to be Forgotten	An admin can search for all incidents by a specific user, then the admin can do a batch operation via the DLP manager user interface to delete the incidents, this will also delete the forensic files associated with the deleted incidents.
Data Storage / Localization	The Incident data storage is Microsoft SQL server is owned by the customer and resides on-premises. The customer can configure encryption settings for the database. Forensics are stored on a network share that is owned by the customer and which resides at the customer premises.

Appendix A

TERMINOLOGY

Term	Explanation
DPS	Data Protection Service – a cloud-based service which runs in Forcepoint AWS account. It uses a Kubernetes infrastructure as well as AWS S3 storage and API gateway. Calling DPS requires a JWT access token
OSS	Object Store Service – a cloud storage that is part of the DPS infrastructure, it uses AWS S3 storage which is exposed as REST API by an AWS API gateway. Calling OSS requires a JWT access token
CASB	Cloud Access Security Broker – a Forcepoint product that connects to customer cloud repositories and services to monitor the customer end-user activities in these cloud repositories and services and enforces security policies.
JWT	JSON Web Token – a string identifier that grants short term access (usually 60 min by default) to other services.