Forcepoint Cloud Data Security Posture Management (Cloud DSPM)

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 representation of warranty, express or implied, and is subject to change without notice. Any refence 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 Cloud Data Security Posture Management?” It is primarily intended for those involved in the procurement and privacy assessment of Forcepoint Cloud Data Security Posture Management.

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://commission.europa.eu/law/law-topic/data-protection_en.

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.

Sub-Processors

Third party provides that may be accessing processing, or storing personal data on behalf of Forcepoint for the provisioning of the relevant Product services.

Name	Description of Service Provided	Location of Processing	Privacy Policy
AWS	Cloud Computing Services	USA	https://aws.amazon. com/privacy
Grafana	Event log storage	USA	https://grafana.com/legal/privacy- policy
Keycloak (self-hosted)	Identity and Access Management Services	USA	https://www.forcepoint.com/company/pivacy-policy
Elastic Search (self-hosted)	Scan meta data store	USA	https://www.forcepoint.com/company/privacy-policy
Mail Chip	SMTP server for sending notification emails to administrators or users of DSPM		https://mailchimp.co m/gdpr

Structure Data

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
Structured database scanning. An administrator configures a database in the DSPM console to scan for sensitive data. The system analyses schemas, tables, columns, views, cells, etc. for sensitive data patterns which may contain personal data.	The data may include personal information (PII. PCI, PHI). Database scanning is performed on the customer's edge environment. Metadata is then sent to the DSPM SaaS platform for summarization and reporting. Sampled database records may be temporarily sent to the DSPM server for classification purposes. This metadata can include schemas, tables, columns, data samples that may contain personal data, as well as information about users and their permissions.	The structured data sources are scanned so that DSPM can discover the objects (tables, columns, views, users etc) associated with the data source and classify them accordingly. This is mainly used to identify where sensitive data resides in an organization to facilitate effective governance, compliance, and data security controls.	No pseudonymization of data is currently available.	Data from structured sources is accessed via a secure ODBC connection. The platform fetches the following information for inspection and classification purposes: • **Database schemas** • **Database object metadata**: including table names, table sizes, number of rows, column names, and column-level metadata • **Column contents**: column data is processed temporarily in memory using the Flink data pipeline solely for classification. Column contents are held in memory for a very short duration and do not persist to disk or stored in the DSPM platform.	The platform does not store raw customer database content. Column data is processed temporarily in memory for classification and does not persist in the DSPM system. Only derived metadata, including database schemas, table names, column names, and classification attributes, are stored in DSPM. Customer configuration data and event-related metadata are retained only while the administrator is actively using the platform. When an administrator leaves the platform, or requests deletion, all configuration and event metadata—including derived structured data metadata—is deleted within 90 business days, or sooner if requested. Note: Although less likely, a table name, column name or any meta data may contain personal information.

How to Manage Subject Access Request (SAR)

SAR – Right Access	Customers can review available metadata through the DSPM console and, where applicable, identify and address any personal information present in the metadata in response to a properly authenticated “Right to Access” request.
SAR – Correction/Rectification	Customers can review metadata through the DSPM console and address any personal information present in the metadata in response to a properly authenticated “Right to Correction/Rectification” request. Any required corrections may involve updating database content directly within the customer’s own database environment, which is outside the scope of DSPM’s direct control.
SAR – Right to be Forgotten	Where a properly authenticated “Right to be Forgotten” request is received, an administrator with appropriate permissions can support fulfillment of the request. Customers can delete the relevant personal data directly within their database, which is outside of the scope of DSPM’s direct control.
Data Storage/ Localization	Database metadata for Cloud DSPM is stored for the duration of the customer’s use of the platform. Currently, metadata is stored in the United States. Additional data storage locations may be supported in the future.

Unstructured Data

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
Unstructured data sources where information is stored in various on-premises or SaaS data stores. Information is typically in the form of files, text, and images. An administrator configures data source connections (ex: OneDrive, SharePoint, SMB fileshare) on the DSPM console to scan for any sensitive data. Any content found within the supported file formats will be analyzed for sensitive data patterns which may contain personal data.	The data may include personal information. Unstructured data source scanning is performed on the customer's edge or in the DSPM SaaS environment. If scanning is done on the customer's edge, metadata is then sent to the DSPM SaaS platform for summarization and reporting. This metadata can include data such as filename, filepath, filetype as well as information about users and their access permissions.	The unstructured data sources are scanned so that DSPM can discover all the files and text messages associated with the data source and classify them accordingly. This is mainly used to identify where sensitive data resides in an organization to facilitate effective governance, compliance, and data security controls. Many unstructured data sources also support DDR scanning – where the scanning happens continuously as users and services interact with the data. DSPM scans can occur on demand or on a schedule. DDR scans automatically get data after being setup. DSPM/DDR scans can classify personal data. Hence the outcomes such as how data is processed, retained, protected or deleted is the same for both types of scans	No pseudonymization is applied to the data. The contents of the files in data sources are never permanently stored or persisted to the DSPM server. Metadata collected is not anonymized.	The system accesses file metadata and file content via authorized APIs for the limited purpose of inspection and classification. File content is processed transiently in memory for a short duration (generally up to 1–2 minutes) and does not persist, is not stored or logged as part of normal system operation. Following inspection, the platform retains only the derived metadata associated with detected events. This metadata may include file paths or identifiers, classification outcomes, sensitivity or compliance-related tags (such as 'PII' or 'PCI'), and related risk attributes. The retained metadata does not include the underlying file contents. However, it is important to note that file metadata may sometimes include personal data. For example, a user's OneDrive folder may contain the username or user email.	The platform does not store the contents of customer files. File contents may be temporarily retrieved in-memory to the DSPM system for classification purposes, and such content is deleted immediately after classification. Customer configuration data and event-related metadata are kept only while the customer is using the platform. When a customer leaves the platform, or requests deletion, all configuration and event metadata are deleted within 90 business days, or sooner if requested.

Unstructured Data Continued

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
				The derived metadata is used to support platform functionality, including dashboards, reporting, and policy-driven alerting. Customers may view file-level metadata and aggregated insights related to data sensitivity, compliance posture, and potential risk. The contents of customer files are not transmitted to or stored on the DSPM platform. Only metadata and classification results derived from the inspection process are collected and transferred, in accordance with the intended system design and data minimization principles. All connections between the DSPM platform and customer data sources are established using secure, encrypted HTTPS/TLS communication. This secure channel is used solely to enable inspection and metadata retrieval. File contents are not transferred from the data sources to the DSPM platform.	.

How to Manage Subject Access Request (SAR)

SAR – Right Access	Customers can review available metadata through the DSPM console and, where applicable, identify and address any personal information present in the metadata in response to a properly authenticated “Right to Access” request.
SAR – Correction/Rectification	Customers can review metadata through the DSPM console and address any personal information present in the metadata in response to a properly authenticated “Right to Correction/Rectification” request. Any required corrections may involve updating database content directly within the customer’s own database environment, which is outside the scope of DSPM’s direct control.
SAR – Right to be Forgotten	Where a properly authenticated “Right to be Forgotten” request is received, an administrator with appropriate permissions can support fulfillment of the request. Customers can delete the relevant personal data directly within their database, which is outside of the scope of DSPM’s direct control.
Data Storage/ Localization	Database metadata for Cloud DSPM is stored for the duration of the customer’s use of the platform. Currently, metadata is stored in the United States. Additional data storage locations may be supported in the future.

Identity Management Data

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
Identity data sources where users' information is stored in various on Prem or SaaS directories or IDP services. An administrator configures identity data sources (ex: AWS_IAM, LDAP, Active Directory, etc.) on DSPM console to scan for user identity information. Any user information and linked file permissions will import to the DSPM system.	The data may include personal information (such as email/usernames). Identity management scanning is performed on the customer's edge or in the DSPM SaaS environment.	To be able to map user permissions to files scanned, view who accessed data and then apply policy actions such as removing access to the users or show policy violations in order to facilitate effective data governance, compliance, and data security controls.	No Pseudonymization is applied to the identity data as this is needed to map to other critical features of the platform such as dashboards, analytics, and policy controls.	The system accesses user login, email information via authorized APIs for the limited purpose of associating users with file permissions. Following user scanning, DSPM maps such information with the data scanned so that administrators can check who owns or has accessed a file. The identity data is used to support platform functionality, including dashboards, reporting, and policy-driven alerting. Customers may view identity data and aggregate insights related to data sensitivity, user permissions, and potential risk. Any user data is retrieved via authenticated APIs and stored securely in the database with access to such data limited to only authorized users.	We store user login and email addresses while the customer is actively using the platform. When a customer stops using the DSPM platform, the customer's tenant, including all associated event metadata and incident logs, is deleted within 90 days, or sooner upon request.

How to Manage Subject Access Request (SAR)

SAR – Right Access	Customers can review available metadata through the DSPM console and, where applicable, identify and address any personal information present in the metadata in response to a properly authenticated “Right to Access” request.
SAR – Correction/Rectification	Customers can review metadata through the DSPM console and address any personal information present in the metadata in response to a properly authenticated “Right to Correction/Rectification” request. Any required corrections may involve updating database content directly within the customer’s own database environment, which is outside the scope of DSPM’s direct control.
SAR – Right to be Forgotten	Where a properly authenticated “Right to be Forgotten” request is received, an administrator with appropriate permissions can support fulfillment of the request. Customers can delete the relevant personal data directly within their database, which is outside of the scope of DSPM’s direct control.
Data Storage/ Localization	Database metadata for Cloud DSPM is stored for the duration of the customer’s use of the platform. Currently, metadata is stored in the United States. Additional data storage locations may be supported in the future.

Endpoint Files

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
End user workspaces where the Forcepoint agent is installed. On the end user workspaces, any file that is opened by an end user may be analyzed for automatic classification or manual classification. Customers can also use the endpoint automatic discovery feature for files to be detected without requiring an end user to open a file. This discovery scans file content and meta data for classification purposes.	Files on end user workspaces may contain personal information. Only metadata information will be stored on the DSPM server. Actual file content is not stored in DSPM. File metadata may also contain PII, in which case, we store such information.	The files on customer workspace are scanned so that such files can be classified automatically or manually. This is done to identify where sensitive data resides in an organization to facilitate effective governance, compliance, and data security controls.	The files on customer workspaces are scanned so that such files can be classified automatically or manually. This is done to identify where sensitive data resides in an organization to facilitate effective governance, compliance, and data security controls.	End user workspace data is processed by the Forcepoint Data Classification (FDC) agent on end user devices. The FDC agent sends file metadata to DSPM. During the classification suggestion process, a part of the file content is sent in an encrypted fashion to DSPM for classification and then immediately discarded (in memory). All connections between the DSPM platform and user endpoints (workspaces) are established using secure, encrypted HTTPS/TLS communication. This secure channel is used solely to enable inspection and metadata retrieval.	The platform does not store end user data files. File contents on endpoints are downloaded in memory for classification on the DSPM system. After the classification is complete, the file content is discarded immediately. Customer configuration data and event-related metadata are kept only while the customer is using the platform. When a customer leaves the platform, or requests deletion, all configuration and event metadata is deleted within 90 business days, or sooner if requested.

How to Manage Subject Access Request (SAR)

SAR – Right Access	Customers can review available metadata through the DSPM console and, where applicable, identify and address any personal information present in the metadata in response to a properly authenticated “Right to Access” request.
SAR – Correction/Rectification	Customers can review metadata through the DSPM console and address any personal information present in the metadata in response to a properly authenticated “Right to Correction/Rectification” request. Any required corrections may involve updating database content directly within the customer’s own database environment, which is outside the scope of DSPM’s direct control.
SAR – Right to be Forgotten	Where a properly authenticated “Right to be Forgotten” request is received, an administrator with appropriate permissions can support fulfillment of the request. Customers can delete the relevant personal data directly within their database, which is outside of the scope of DSPM’s direct control.
Data Storage/ Localization	Database metadata for Cloud DSPM is stored for the duration of the customer’s use of the platform. Currently, metadata is stored in the United States. Additional data storage locations may be supported in the future.

Appendix A – Terminology

Cloud DSPM	Forcepoint Data Security Posture Management (DSPM) helps organizations quickly find, classify, and secure sensitive data across cloud and on-prem environments. With high-speed scanning, AI powered classification, and full visibility into data access, Forcepoint DSPM reduces risk, improves compliance, and strengthens overall data protection.
Structured Data	Data/information organized in defined, tabular formats—typically rows and columns within relational databases such as MySQL, PostgreSQL, Oracle, Microsoft SQL Server, and IBM DB2.
Unstructured Data	Non-tabular content that doesn't conform to a rigid schema—such as documents, emails, spreadsheets, files, and media stored across on-premisesor cloud environments.
Endpoint Data	Data files on customers' end users' workspaces and assets (e.g., laptops/computers) where the Forcepoint Endpoint agent is installed.
Identity Data	User identity data (e.g., usernames, email address) from sources (e.g., LDAP, Microsoft AD, AWS_IAM, etc.) that are configured by customer DSPM administrators.
User	Individual (e.g., customer employees) that has the Forcepoint Endpoint agent installed and running in their workspace or on their assets (e.g., laptops/computers).

Forcepoint

About Forcepoint

Forcepoint enables Self-Aware Data Security, an AI-native approach that helps enterprises and governments know their data everywhere, adapt to evolving risks and regulations in real-time, and protect at scale with a unified, single-policy framework. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, LinkedIn, Instagram and YouTube.

[Forcepoint DSPM (Cloud DSPM)] [Status]26 Jan. 26