VECTRA

Vectra Recall Privacy Datasheet

This Privacy Datasheet describes the personal data processed by Vectra Recall offering (“Recall”).

Vectra Recall Overview

Vectra Recall solution is a cloud service which stores historical network metadata from customer’s deployed Vectra AI Network Detect and Response appliance in support of security investigations and threat hunting.

The types of personal data processed by Vectra Recall

The following table shows the personal data processed by Vectra Recall, and the purpose for processing such personal data.

Personal Data Source	Personal Data Type	Examples of Personal Data	Purpose for Processing
Network Data	Client and server hostnames	Example: jane-doe-laptop	To (i) provide detection and response services to protect customer environments; (ii) conduct investigations into events impacting customer environments to resolve technical issues and (iii) optimize and improve the performance of Vectra AI products and services.
	Source IP and destinations address	Example: 53.1.1.1	
	URL, cookie, referrer, user agent	Example: http://www.vectra.ai?user=janedoe	
	SMB files and mappings	Example: \\server\jane-doe-report.doc	
	RDP Cookie	Example: janedoe	
	MAC Address	00:21:44:23:45:67	
	AD and LDAP user information	DC=corp,DC=ai, CN=John* givenName=-Jane Doe	
	AD Realm names	corp.ai	

*Only processed if the contents of the associated email are identified as related to a possible security threat by Microsoft’s native reputation engine.

Who can access the personal data processed by Vectra Recall

The table below sets forth who can access personal data, and the purpose of the access.

Personal Data Source	Who Has Access	Purpose of the Access
Network Data	Customer	To provide customer access to Network Data for security investigations and threat hunting;
	Vectra AI	To (i) provide detection and response services to protect customer environments; (ii) conduct investigations into events impacting customer environments to resolve technical issues and (iii) optimize and improve the performance of Vectra’s products and services.

How Vectra AI secures personal data processed by Vectra Recall

Vectra AI has implemented technical and organization security measures in order to preserve the confidentiality, integrity and availability of personal data, including pseudonymization of all Network Data processed by Recall when the Sharing Metadata feature is enabled.

Personal Data Source	Security Measures
Network Data	Data in transit is encrypted using a secure TLSv1.3-encrypted session. Data at rest is encrypted using Cryptographic Service Provider (CSP) techniques.

Vectra Recall personal data retention and deletion practices

Vectra Recall personal data retention practices and the purpose for such retention are set forth below.

Personal Data Source	Retention Period	Purpose of Retention
Network Data	**By Customer:** Customer may purchase a Network Data retention period of two (2), four (4) or twelve (12) weeks. Network Data will be deleted once the applicable purchased retention period has expired.	**By Customer:** To (i) provide customer access to Network data for security investigations and threat hunting; (ii) conduct investigations into events impacting customer environments to resolve technical issues; (iii) optimize and improve the performance of Vectra AI's products and services.
	By Vectra AI: Network Data will be retained for the retention period purchased by customer, and will be deleted once the applicable purchased retention period has expired.	**By Vectra AI:** To (i) provide detection and response services to protect customer environments; (ii) conduct investigations into events impacting customer environments to resolve technical issues and (iii) optimize and improve the performance of the products.

Portability of personal data processed by Vectra Recall

Data may be exported from Vectra Recall by the customer through the Recall UI (user interface).

Data center locations where Vectra Recall processes personal data

Personal data may be stored in the following data center locations. When Sharing Metadata is enabled, regardless of the selection of a regional data center, pseudonymized Network Data will be processed in the United States to optimize and improve the performance of Vectra AI products and services. Since the Remote Support feature offers viewing/access capability only, no personal data is transferred to a Vectra AI data center location..

Personal Data Source	Data Center Provider	Data Center Location	
Network Data	AWS	Customers have the ability to select one of the following regional data center locations:	
		• United States • Canada • France • Germany • Ireland • United Kingdom	• India • Bahrain • UAE • Australia • Japan • Singapore

Vectra Recall Sub-processors

Vectra AI utilizes the following subprocessors to provide the Recall offering. All subprocessors must meet the same security posture as Vectra AI, and have a data protection agreement in place with Vectra AI. For customers who have enabled the "Sharing Metadata" feature, personal data will be processed in the United States regardless of the selection of a regional data center location (where available).

Sub-processor	Personal Data Source	Service Provided	Data Center Provider/Location	
AWS	Network Data	Cloud Infrastructure	Customers have the ability to select one of the following regional data center locations:	
			• United States • Canada • France • Germany • Ireland • United Kingdom	• India • Bahrain • UAE • Australia • Japan • Singapore
Databricks	Network Data	Cloud Analytics	Customers have the ability to select one of the following regional data center locations:	
			• United States • Canada	• Ireland • Australia

Compliance

Data Processing Agreement/Data Subject Access Rights

Vectra AI processes all personal data in accordance with Vectra AI's Data Processing Agreement ("DPA"). Vectra AI upholds its obligations as a processor, and, pursuant to the DPA, provides applicable assistance to support customer responses to data subjects' requests to exercise their rights under applicable data protection laws.

Security Certification

Vectra Recall is a SOC2-audited service built on top of AWS. We have completed a SOC2 type 1 report, have implemented all required controls, and have successfully completed a SOC2 type 2 audit. For more details on our compliance, or to obtain a copy of our SOC2 type 2 audit report, please visit Vectra's Trust Center.