GDPR Compliance

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Oded David & BDO	Initial Version		11/10/2020
2.0	Shiran Wolfman	Revised all sections		05/11/2021

Table of Contents

Table of Contents

1.0 Background

2.0 Scope

3.0 Measures for Risk Mitigation

4.0 Mechanisms to Ensure Protection of Personal Data

5.0 Data Subject Requests

6.0 Organizational and Administrative Security Measures and Controls

7.0 Technical Security Measures

8.0 Additional Information

1.0 Background

On May 25th 2018 the EU's General Data Protection Regulation came into effect in order to strengthen the privacy of individuals' personal data.

Coralogix complies with applicable data protection regulations including our regulatory requirements under GDPR. Coralogix acts strictly as a Processor as defined in GDPR article 1. Processing takes place lawfully, fairly and in a transparent manner. Our platform and services process data in a framework that ensures the privacy and security of our customers' data.

2.0 Scope

Coralogix direct customers are companies rather than individuals. Coralogix's services are not explicitly intended to be used for processing personal data of customers or their customers. We process customers' data strictly for the stated purpose and do not monetize on, or sell data received to third parties. Coralogix treats the data it receives from customers as a black box, i.e. there is no way for Coralogix to pick a customer and run a query as this would require a schema over their logs. The data on Coralogix's systems, in its sensitive form, is de-facto irretrievable by Coralogix and only the customer knows how to make sense of it.

3.0 Measures for Risk Mitigation

Coralogix provides customers with the tools to filter and mask personal data in logs before sent to us for processing. Our Customer Success team provides extensive assistance to customers in setting rules for anonymizing personal data. If a customer feels that they may have leaked personal information to us in logs we will, with their explicit consent and direction (and under a supervised pre-defined process), make our best efforts to delete such logs.

4.0 Mechanisms to Ensure Protection of Personal Data

Coralogix gives customers the ability to choose the location in which their data is hosted in order to comply with data residency requirements under the GDPR. Coralogix tracks adequacy decisions of regulatory bodies and ensures strict compliance of data flows. We maintain extensive technical and organizational safeguards.

Although Coralogix services are not explicitly intended for the processing of personal data, we have published and made available our Data Protection Agreement for any customer who wishes to sign. The standard data protection clauses include the updated SCC's for the purpose of ensuring compliance with required cross-border transfer restrictions where applicable.

5.0 Data Subject Requests

We support our customers in meeting their obligations towards data subject requests whether in deleting personal data that may have been processed or in providing a clear report with requested information. We may also assist customers with their obligations towards inquiries by regulators in the context of their use of Coralogix's services.

6.0 Organizational and Administrative Security Measures and Controls

Coralogix maintains policies and procedures in order to maintain, implement, administer and audit our security, and to ensure the ongoing confidentiality, integrity and availability of processing systems and services. Policies and Procedures are audited annually by external auditing firms and affirmed by our passing of recognized certifications and standards such as SOC 2 and ISO 27001/27701 (amongst others as detailed in our security/compliance page).

7.0 Technical Security Measures

Internal Level

Coralogix maintains several internal measures to protect our systems from breach including a comprehensive vulnerability management program, quarterly penetration testing by qualified 3rd parties, network security measures, MFA for all privileged software and infrastructure access, access control measures, threat intelligence measures, threat detection, SDLC security measures.

Customer Level

Data Encryption

Coralogix encrypts customers' data both at-rest and in-transit. If a customer stores their logs in a cloud object storage bucket that they control, then they have full control over the bucket-layer encryption used within that bucket. Logs stored on Coralogix servers are encrypted at rest with AES-256. Logs sent to Coralogix are encrypted in transit with TLS 1.2.

Data Sovereignty

Coralogix allows Customers to have complete control over their logs by storing their logs into an object storage bucket (AWS S3 supported) in a cloud account that they control. Because customers own the object storage bucket and the cloud account which hosts it, they retain full control over access management to that bucket and can revoke access at any time.

Data Stillness

Once customers' logs are stored on their cloud object storage bucket, Coralogix indexes and searches their data directly from theirbucket, without keeping a local copy of their logs. Once customers' logs have been written to their bucket, they are gone from Coralogix's systems. This ensures strict compliance with data protection regulations as it keeps customers' logs much more private and secure compared to competing solutions that requires keeping the full logs on datastores.

User Account Access Control

Part of our security measures include customer-defined permissions via identity management. Coralogix provides a detailed audit trail for all activities within the Coralogix platform.

When you create a team in Coralogix, you can create personal accounts for each of your employees in the team. Coralogix supports single-sign-on (SSO) from an identity provider (IdP) that supports SAML login. Coralogix also supports automatic provisioning and deprovisioning of user accounts with SCIM. Additionally, Coralogix provides a detailed audit trail for all activities within the Coralogix platform.

Role-Based Access Control (RBAC)

Granular, role-based access control (RBAC) enables customers to control the actions a user can perform within the Coralogix platform and restrict access to only a user's relevant logs. Coralogix RBAC also supports assigning users into multiple groups while still allowing different action permissions to any subset of users.

8.0 Additional Information

If you have any questions regarding Coralogix's compliance with GDPR you may contact our Data Protection Officer. For a comprehensive list of our policies, procedures, certifications and security controls you may visit our Security & Compliance Page.