New Relic
EU Data Protection Whitepaper

November 2015

New Relic, Inc.
188 Spear Street
San Francisco, CA 94105

Table of Contents

I. Introduction

This document (or "Whitepaper") is intended to provide a high-level overview of the New Relic Security and how it helps our customers manage compliance with relevant data protection laws. It addresses the most common concerns customers may have about security and privacy, particularly in the European Union ("EU"), and outlines the security controls and mechanisms provided by New Relic which relate to data processing.

II. Purpose

This Whitepaper aims to help customers understand:

- What measures New Relic takes to protect the security and privacy of our customers' data
- How New Relic allows its customers to retain control over the data they choose to send us
- The respective responsibilities of New Relic and our customer in managing and securing content sent to and processed by New Relic

More specifically, it will answer the following commonly asked questions:

- What type of data does New Relic process on behalf of customers?
- How will the data processed by New Relic be secured?
- What controls do customers have on the data they process in connection with the services?
- Where will the data be stored?
- Who will have access to the data?
- How long does New Relic retain data?

So let's dive in!

III. Overview of Directive 95/46/EC

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (also known as the "Directive") sets forth a number of data protection requirements which apply when "personal data" about an identified or identifiable individual (referred to as a "data subject") is being "processed," as such terms are defined in the Directive.

In the context of New Relic's services, the customer determines the purpose and means of processing of personal data and is therefore the "data controller" under the Directive. New Relic, as the entity which processes personal data on behalf of and at the direction of the data controller, is the "data processor."

Through its provision of the services, New Relic provides a technical means by which our customers may transmit and process their data, therefore enabling our customers to direct what data is processed. Accordingly, the data transmitted and processed may include personal data, if our customer so chooses. Accordingly, New Relic does not have visibility into or actual knowledge of what customers are processing through its use of the services, including whether or not the data processed includes personal data.

Under the Directive, it is the responsibility of the data controller to ensure that, if it chooses to process personal data, its processing of personal data is compliant with data protection obligations. It is also the data controller's responsibility to ensure that appropriate technical and organizational measures are used to protect personal data from accidental or unlawful destruction or loss, alteration, or unauthorized disclosure or access. Where processing is carried out by a data processor on a data controller's behalf, the data controller is also responsible for choosing a data processor that provides sufficient technical and organizational measures governing the processing of the categories of data they choose to process.

IV. New Relic and Compliance with Directive 95/46/EC

New Relic aims to empower its customers to use the New Relic services in a way that maximizes the value of our offerings while remaining mindful of relevant data protection obligations. This Whitepaper will provide details with respect to New Relic's services and how customers process data using the services.

Comprehensive details on New Relic's services in the context of the Data Protection principles set forth by the Directive can be viewed here.

Please note that this document is merely intended to provide informational guidance on New Relic's services in the context of the Directive. Customers should bear in mind that the Directive may not apply to organizations established in certain EU Member States where differing national laws may be applicable. Further, this document does not address all privacy and data protection laws and regulations which may be applicable to individual customers, as this may depend on different factors, including, but not limited to, where and how a customer conducts its business and chooses to use the services, the industry in which the customer operates, and the type of data a customer may choose to process.

1. Types of Data Processed By Default

New Relic's services process performance data for the applications or servers on which our client-side software (referred to as a "New Relic Agent") is installed in order to provide the services. Generally, this includes information such as aggregate time measurements for application transactions, performance data on web page loading, application errors and transaction traces, and server resource utilization statistics.

This means that, by default, personal data is not processed through the New Relic services. Certain customers may choose to configure the New Relic's services to process other types of data for their use, including some forms of personal data. This is completely within the customer's control. However, regardless of whether not a customer chooses to process personal data using the services, New Relic is committed to the security of our customers and their applications, and have designed technical controls into our offerings to help customers maintain the security of their data.

2. Purposes of Data Use

The data processed by New Relic at the direction of our customers is used for the following purposes related to its provision of Services:

- Personal data of our Customer's New Relic account users (including first and last name, email address, and job title) is used to administer New Relic's services, for example, to provide log-in access or to communicate with the New Relic account users about their use of the services.
- Data processed via the services on behalf of our customers (application data) is used to display application performance information back to the Customer's New Relic account user.

3. Subcontractors or Sub-Processors

New Relic uses certain third party subcontractors (or "sub-processors") to assist in our provision of the services. This includes, but is not limited to, subcontractors who:

- Provide communication tools enabling New Relic to email our customers or respond to our customers' support requests
- Provide hosting solutions as part of New Relic's provision of services
- Provide payment processing solutions

New Relic maintains contractual safeguards to ensure that relevant industry standard data protection mechanisms are maintained for these subcontractors.

4. Data Storage

Data processed via the New Relic services is hosted in the U.S. at a secure Tier 3, SOC 2-certified data center. Some application data is also stored at New Relic's secondary location hosted by AWS, which is also a secure tier 3 SOC 2-certified data center. Application data hosted by New Relic does not leave the US.

5. Access Controls

New Relic employs a strict, role-based access control framework to restrict employee access to application data. Access to application data is granted solely where an employee's job responsibilities necessitate access to application data on a strict, need-to-know basis. In order to ensure compliance with our access control policies, New Relic conducts quarterly access audits. Breaches and inconsistencies are investigated and remediated as discussed in Breach Response section below.

6. Data Retention

Retention of application data is dependent upon the particular level of service purchased from New Relic, up to a period of 90 days. Upon termination of the New Relic services, application data is expired out of New Relic's systems (including backups) within a commercially reasonable period of time, but no more than 90 days.

7. Certifications

New Relic is SOC 2, Type II-certified, and undergoes an audit

process annually to provide ourselves and our customers with independent, third-party assurances that New Relic is maintaining industry standard processes and are taking the appropriate steps to protect our systems.

New Relic is also a member of the Cloud Security Alliance (CSA) and has proudly published the results of our Security, Trust & Assurance Registry (STAR) self-assessment on the CSA website. These results include detailed information about New Relic security controls can be found at https://cloudsecurityalliance.org/star/.

Conclusion

New Relic is trusted by 500,000 users and 12,000 paid business accounts to provide secure, world class software analytics services. To serve this broad and dynamic customer base, which includes customers of all sizes and across all industries, maintaining the security of our services and managing the privacy concerns of our customers are our top priorities.

To further understand how to address security and privacy, customers are encouraged to read the materials, best practices, and other guidance that is made available on the New Relic website. This material can be found at https://docs.newrelic.com/. If you require further information, please contact your New Relic Account Executive or visit https://support.newrelic.com/.