New Relic

May 2018

General Data Protection Regulation (GDPR) FAQ

At New Relic, we understand the importance of data. Our privacy and security professionals have been working with customers and internal teams to prepare for the GDPR, which became effective May 25, 2018. We know our customers, especially those in the European Economic Area (EEA) or processing data from the EEA, care deeply about the privacy and security of the performance data transmitted to New Relic for processing. Similar to existing legal requirements, compliance with the GDPR requires a partnership between New Relic and our customers in the use of our services. New Relic has taken steps to enable our customers who elect to process personal data in our products to do so in accordance with the GDPR and applicable data protection laws, and we work to ensure that our practices and contracts are prepared to support EEA customers who wish to include personal data in their performance data.

Does New Relic process personal data as part of performance data?

Our software agents are not designed to write any personal data to file by default. Our products are focused on the performance of software, systems and applications - not individuals. However, if a customer wishes to set up a custom API, custom attribute, or custom event to track such personal data, it may do so, subject to the terms and conditions of the customer's agreement with New Relic (i.e. the customer is contractually restricted from sending us personal health information, government issued identification numbers, financial account information, and sensitive personal data as defined under the GDPR). Our processing is data agnostic and automated, so all data will be processed in the same way in accordance with our customer's particular configuration.

How does New Relic process performance data?

For **Infrastructure**, **Browser**, **Mobile**, and **APM**, once a customer installs the New Relic software agent in the software, system, or application they wish to monitor, the agent will transmit performance data to New Relic servers, where it is processed. **Synthetics** uses automated scripts to test a customer's software, systems, and applications; these scripts sit on AWS servers or customer locations and report data back to New Relic servers. **Insights** enables deeper data analysis into performance data from Infrastructure, Browser, Mobile, APM, and Synthetics or from other sources via a custom API set up by the customer.

Where are New Relic's servers? What mechanisms do you use to adequately transfer data from the EEA to the US?

We host our applications and serve all our customers from data centers located in the Chicago, Illinois area and, to a lesser extent, a combination of cloud hosting providers. If you require more specific details, you can contact your Account Executive for a copy of our SOC 2 Report, which is released under a separate nondisclosure agreement. For entities in the EEA to send personal data outside of the EEA, an adequate transfer mechanism must be used. New Relic is both EU-US and Swiss-US Privacy Shield self-certified (https://newrelic.com/privacy-shield) and we enter into standard contractual clauses upon request. Both Privacy Shield and standard contractual clauses are considered adequate mechanisms of transfer. See below for more information.

Data Protection Addendum, Standard Contractual Clauses and Privacy Shield

New Relic has been working to ensure its contracts are prepared to support EEA customers who wish to include personal data in their performance data. We currently offer compliant data protection addendums (DPA) for customers preparing for the GDPR that include standard contractual clauses (an adequate mechanism for transfer of Personal Data). In addition,New Relic is both EU-US and Swiss-US Privacy Shield self-certified (https://newrelic.com/privacy-shield). Please reach out to your Account Executive for more information.

New Relic

May 2018

What security measures has New Relic taken to protect performance data?

Our security teams continue to ensure we are in line with industry standards and best practices when it comes to performance data. By default, data is encrypted in transit from the agent to New Relic's servers. New Relic's servers sit in a Tier III, SOC 2 data center and New Relic undergoes annual SOC 2 Type II audits of its security practices and policies, the results of which are made available upon request.

How will New Relic respond to data subject requests for deletion of personal data?

New Relic has done extensive data mapping of personal data in accordance with the GDPR. We do provide deletion request support based on subscription level. For more information on how to submit a deletion request based on the type of your account see: https://docs.newrelic.com/docs/using-new-relic/new-relic-security/security/new-relic-gdpr-deletion-requests. Or, submit a Personal Data Request Form https://newrelic.com/content/dam/new-relic/privacy/personal-data-request-form.pdf to PersonalDataRequests@NewRelic.com.

What about other data subject requests?

For all other data subject requests, please submit a Personal Data Request Form https://newrelic.com/content/dam/new-relic/privacy/personal-data-request-form.pdf to PersonalDataRequests@NewRelic.com. If you are confused about what data subject rights are, see Section 4(vii) of our revised Privacy Policy, a link to which you can find below.

Has New Relic appointed a Data Protection Officer?

Yes, New Relic has decided to appoint two Data Protection Officers. An internal Data Protection Officer, Shaun Gordon, our Chief Security Office and Chief Privacy Officer. And an external Data Protection Officer based in Germany. To contact either, please email: AskPrivacy@newrelic.com.

Due to the complexity and fast moving pace of New Relic's product development, Shaun Gordon's internal DPO role is to ensure sufficient internal oversight is provided for Data Protection Impact Assessments in both our product and vendor reviews and privacy by design/default processes. Privacy review has been added to the extensive security review processes already in place.

In addition, New Relic has Privacy and Product Counsel (aka an attorney) at the product headquarters in Portland, Oregon to work with the product teams in their privacy compliance, as well as Privacy Counsel in the European headquarters in Dublin, Ireland.

This document will be updated periodically as we receive additional questions from our customers.

For additional information see:

New Relic Privacy Policy: https://newrelic.com/termsandconditions/privacy
New Relic Cookie Policy: https://newrelic.com/termsandconditions/cookie-policy
New Relic Terms of Service: https://newrelic.com/termsandconditions/terms
GDPR Deletion Requests: https://docs.newrelic.com/docs/new-relic-gdpr-deletion-requests
Personal Data Request Form:
https://newrelic.com/content/dam/new-relic/privacy/personal-data-request-form.pdf
New Relic Cookies Used by Browser:
https://docs.newrelic.com/docs/browser/new-relic-browser/page-load-timing-resources/new-relic-cookies-used-browser