

General Data Protection Regulation (GDPR) FAQ

At New Relic, we understand the importance of data and its protection. Our privacy and security professionals collaborated with customers and internal teams to prepare for the GDPR, which went into effect 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. Compliance with the GDPR requires a partnership between New Relic and our customers in the use of our services. New Relic enables 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 any customers who wish to include personal data in their customer data (data that New Relic collects and processes on behalf of its customers as defined in the [Terms of Service](#) or customer contract).

Is New Relic compliant with the European Union's GDPR?

With regards to the processing of customer data, New Relic acts as a data processor (under GDPR); in other words, New Relic does NOT generally determine the purpose and means of processing and is

therefore not in a position to make any statement about compliance. When New Relic acts as data controller (i.e. when New Relic does in fact determine the purpose of processing such as when we process account data or audit logs), New Relic complies with all applicable laws. Moreover, New Relic will endeavor to take as consistent a position as possible regardless of the individuals' country of residence or region of origin. For more information see [Compliance with legal requirements](#) in the online documentation.

Does New Relic process personal data as part of the customer data?

New Relic agents do not collect personal data by default with limited exceptions¹. Our products are focused on the performance of software, systems and applications - not individuals. Customers may configure custom APIs, custom attributes, or custom events to track personal data, subject to the terms and conditions of their agreement with New Relic. Our processing is data agnostic and automated, so all data is processed in the same way in accordance with each customer's configuration and instructions.

¹The Browser and Mobile agents collect the IP address of the client device to derive high-level geographical information (city, state, country). This IP address is not stored permanently in performance data. Additionally, the Mobile agent collects a New Relic-specific unique deviceID for billing purposes.

Does New Relic process special categories of data?

No, New Relic's [terms of services](#) and customer contracts specifically prohibit the use of the services to collect, process and store special categories of data as defined in the EU GDPR.

Where are New Relic's servers?

New Relic processes and stores all performance data either in our US or EU region as selected by each customer, and uses backup data centers in these same regions for disaster recovery. For more information see [Our EU and US region data centers](#) in the online documentation.

What contractual mechanism does New Relic use for data protection?

New Relic contracts are designed to support customers who wish to include personal data of EU data subjects in their customer data. To ensure that an adequate mechanism is in place for all transfer of personal data outside of the EEA, New Relic self-certifies with both [EU-US and Swiss-US Privacy Shield](#) and can enter into standard contractual clauses upon request.

New Relic's data protection addendum (DPA), which customers may request, includes standard contractual clauses. Please reach out to your Account Executive for more information.

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

Our security teams continue to ensure we are in line with industry standards and best practices for all data processing. By default, data is encrypted in transit between the agent and New Relic's servers, which are housed in Tier III, SOC 2 data centers, and at rest as documented in the online [help](#). New Relic undergoes annual SOC 2 Type II audits of its security practices and policies, the results of which are made available upon request.

Can New Relic delete or return customer data?

Customers can request help with deletion of their data at any time. Upon closure of a customer account, all customer data is deleted within 90 days. Requests for return or deletion of data are handled on a case by case basis.

How will New Relic respond to data subject requests?

New Relic has well defined processes to respond to data subject requests, including consent, documented in [Personal Data Requests](#).

Should New Relic receive a request from a customer's customer, we will promptly forward it to the appropriate customer.

Has New Relic appointed a Data Protection Officer?

Yes, New Relic appointed two Data Protection Officers. An internal Data Protection Officer, to ensure sufficient internal oversight for Data Protection Impact Assessments, product and vendor reviews

and privacy by design/default processes, and an external Data Protection Officer based in Germany. To contact either, please email Privacy@newrelic.com.

In addition, New Relic has a Privacy and Product legal team with presence both in the USA offices and in its 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 General Privacy Notice](#)
- [New Relic Services Privacy](#)
- [New Relic Cookie Policy](#)
- [New Relic Terms of Service](#)
- [Personal Data Requests](#)