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 EU GDPR/UK 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 EU GDPR/UK 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 Services or customer contract).

Is New Relic compliant with the European Union’s GDPR and the United Kingdom’s GDPR?

With regards to the processing of customer data, New Relic acts as data processor (under the EU GDPR/UK GDPR); in other words, New relic does NOT generally determine the purpose and means of processing. Where New Relic acts as a data processor, we comply with our obligations as a data processor under the EU GDPR/UK GDPR.

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 operates in a data and industry agnostic B2B environment whereby companies send telemetry data about technologies to New Relic. New Relic’s services are designed to receive and process telemetry data on the performance of applications, systems, networks and infrastructure and are primarily focused on the performance of software—not individuals. New Relic customers have access to the New Relic platform which is built around the four fundamental telemetry data types necessary for complete and effective system monitoring: metrics, events, logs, and traces ("MELT" data). New Relic Browser and Mobile temporarily process IP addresses for the purpose of deriving a city and state and are then subsequently discarded. Otherwise by default, New Relic’s agents for metrics, events and traces do not collect any personal data— it is possible for New Relic customers to customize and configure metrics, events and traces to transmit personal data to the New Relic services for processing but this is within each customer’s sole control. If you are concerned about the transmission of personal data through metrics, events and traces, you can just choose to change your own systems and software to not send it. Logs are treated differently due to the nature of their content. Unlike metrics, events and traces, logs consist of unstructured data generated by the customer’s various systems
and largely from and about those systems. Systems that are designed to process personal data are likely generating logs that will contain personal data. Monitoring those systems with New Relic may cause New Relic to collect such personal data in logs on your behalf. If you prefer not to have your APM logs collected and processed by default, New Relic makes a toggle switch available to all customers in the New Relic user interface (UI) which will enable you to easily and quickly turn off logs from the APM agents at the New Relic Account level. Once this is done, no personal data will be transmitted via New Relic Logs.

For more information, please see https://docs.newrelic.com/docs/logs/logs-context/disable-automatic-logging/

Even though it is not necessary to transmit personal data to New Relic in order to use the Services, you can and should feel comfortable sending data to us. New Relic is an EU GDPR /UK GDPR compliant data processor and has incorporated the new 2021 Standard Contractual Clauses (SCCs) into the New Relic DPA and has restructured its security exhibit to align with the 2021 SCCs to make your review of our safeguards easier. Additionally, New Relic has obtained certifications from independent, third-party auditing organizations such as ISO27001 and HITRUST and provides security in accordance with industry accepted standards described here. If you do accidentally transmit any personal data, you can rest assured that New Relic has sufficient protections in place to safeguard that data and you may also submit a request to have that data deleted as described here.

Does New Relic process special categories of data?

No, New Relic’s Terms of Service 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/UK 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/UK 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, Switzerland and/or the United Kingdom, New Relic has a pre-signed EU GDPR/UK GDPR Customer DPA available here which incorporates: (i) the new Standard Contractual Clauses for the transfer of personal data as per the European Commission’s Implementing Decision 2021/914 of 4 June 2021 for EU GDPR transfers and (ii) an equivalent transfer mechanism for UK GDPR transfers. Additionally, although the EU-US and Swiss-US Privacy Shield frameworks were both invalidated as a personal data transfer mechanism in 2020, New Relic is still obliged by the US Department of
Commerce to comply with our obligations under the Privacy Shield in order to maintain our existing Privacy Shield certification.

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. Additionally, New Relic has obtained certifications from independent third-party auditing organizations such as ISO27001 and HITRUST and provides security in accordance with industry accepted standards described here.

Can New Relic delete or return customer data?

Customer 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 Assessment, 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 our European headquarters in Dublin, Ireland.

The 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