

Achieving GDPR Compliance with GoodData

On May 25, 2018, the General Data Protection Regulation (GDPR) 2016/679 will come into effect. Designed primarily to give European Union citizens and residents control over the use of their personal data, GDPR will require companies to rethink the way they store and use data for business purposes. Ahead of the official enforcement date, GoodData is sharing the preparations we've taken and addressing some common customer questions.

How is GoodData preparing for GDPR?

As the leader in cloud-based Business Intelligence and Embedded Analytics, GoodData recognizes the responsibility to enable its customers to comply with the emerging legislation. In addition, as a global company, GoodData needs to ensure adequate protection of personal data of its European employees, customers and their clients, partners, vendors, and other EU-based individuals who are involved with GoodData.

To prepare, GoodData initiated its GDPR compliance project in March 2017, more than a year ahead of the compliance deadline. Since then, GoodData has devoted considerable time, human capital, and monetary resources to achieving compliance with this important regulation. The experience, insight, and knowledge gained during this process have strengthened GoodData's security and privacy practices for the benefit of its customers, partners, suppliers, and employees now and into the future.

What did GoodData do to become compliant?

GoodData values and honors the individual's right to privacy, and many of the precautions required for GDPR were already in place. Consequently, the impact of GDPR on the GoodData services offering and business processes was rather small. We comply with the existing 95/46/EC Data Protection Directive (predecessor to GDPR), and we participate in the International Trade Administration's US-EU and US-Swiss [Privacy Shield Framework](#). GoodData has also leveraged its experience with ensuring security and privacy of highly sensitive electronic protected health information (ePHI).

GoodData's specific GDPR compliance efforts addressed the following areas:

- Establishing an overall privacy management program
- Ensuring compliant processing of customer data in the GoodData platform
- Ensuring compliant processing of personal data as part of GoodData's business operations

- Ensuring compliant processing of the personal data of GoodData's EU employees

We have also taken the opportunity to expand our existing privacy and security standards outside of the GoodData platform, converted best practices into formal policies and processes, made our information security practices even more robust by implementing ISO 27001:2013 compliance, and prepared records of processing activities as required by [Art. 30 GDPR](#). We have also updated our data processing agreement to comply with [Art. 28 GDPR](#) requirements.

Finally, as our customers or their clients are the data controllers of personal data processed in the GoodData platform, they need to ensure their solution is compliant. To support our customers in this endeavor, GoodData has prepared implementation guidelines so our Professional Services team can ask the right questions to help our customers make their solution comply with GDPR.

What impact will GDPR have on GoodData customers?

Many GoodData customers will be affected by GDPR at least to some extent. However, the impact of GDPR will vary by customer and depends heavily on how the GoodData platform is used and the nature of the business, as well as the scope and extent of personal data that is processed.

We encourage all customers who are subject to GDPR to take the following steps:

1. Review your privacy policy, terms of use, or similar documentation to ensure the individuals whose data you are processing are adequately informed, as required by [Art. 12 GDPR](#).
2. Whenever you collect data directly from individuals, you should provide them with a privacy notice ([Art. 13 GDPR](#)). If you obtain data from other sources or companies, you need to ensure individuals are informed about the collection of their personal data, as required by [Art. 14 GDPR](#).
3. You might need to sign a formal data processing agreement with us. We are happy to do so and have ensured that the agreement complies with GDPR requirements. Ask your account manager to guide you through the process.
4. Depending on your business scenario, you might want to review your solution in the GoodData platform to ensure it complies with the guidelines for processing personal data ([Art. 5 GDPR](#)), particularly with respect to data minimization and storage limitation requirements, and that you can easily respond to data subject privacy requests as required by [GDPR Chapter 3](#). Should you require any assistance, please ask your account manager.

Frequently Asked Questions

We have personal data for EU residents in GoodData's US datacenter. Do we need to move it to the EU?

While GoodData offers an EU datacenter and recommends that its European customers use it, GDPR [does not prohibit moving personal data outside of the EU/EEA](#), provided that [certain criteria are met](#). GoodData also participates in the International Trade Administration's US-EU and US-Swiss [Privacy Shield Program](#) and will enter into Standard Contractual Clauses with its customers, so personal data of EU residents may remain in GoodData's US datacenter, even under GDPR.

What are the "Special Categories of Data"? Can we analyze them in the GoodData platform?

Defined in [Art. 9 GDPR](#), Special Categories of Data are highly sensitive personal data that relate to fundamental rights and freedoms, such as information related to individual health, sex life and orientation, racial or ethnic origin, religion, beliefs, political opinions, union membership, and others.

By default, GDPR prohibits the processing of such data unless specific criteria are met. However, if GoodData customers have legitimate grounds for processing this data, we are ready to assist you and have established protocols for ensuring security and privacy. Please inquire with your account manager or account executive about our GDPR Compliance Services for Special Categories of Data.

Has GoodData appointed a Data Protection Officer?

Because the processing of personal data actually performed by GoodData is relatively limited compared to the significant amount of data and technical capacities at its disposal, GoodData is not obliged to appoint a DPO as defined in [Art. 37 GDPR](#). This was confirmed by external legal counsel and validated by the Data Protection Authority. However, GoodData has appointed a Privacy Officer, who oversees GoodData Privacy Management system and serves as an escalation point for all privacy-related requests, inquiries, and complaints. You can contact the GoodData Privacy Officer at privacy@gooddata.com.

How can customers confirm that GoodData provides sufficient privacy guarantees?

Under [Art. 28 GDPR](#), the Controller, which is either GoodData's customer or their clients, shall use only processors that provide sufficient guarantees that data processing will meet GDPR requirements and ensure the protection of the rights of the data subject.

GoodData customers may validate GoodData's security measures by reviewing GoodData's SOC 2 Type II audit report and additional security compliance documentation. Upon request, GoodData will also provide its customers an overview of all subprocessors and demonstrate the contractual arrangements that are in place to ensure sufficient guarantees are established.

Subject to the terms of the data processing agreement and as required by [Art. 28 GDPR](#), GoodData will also provide any additional documentation necessary for demonstration of compliance and will assist in customer compliance audits and inspections.

How can an individual contact GoodData about privacy measures?

GoodData has established a dedicated [e-mail address](mailto:privacy@gooddata.com) for all privacy inquiries: privacy@gooddata.com. Should an individual inquire about data processed in our platform by a GoodData customer, we will promptly inform the customer and will not act upon the request unless specifically required by law or authorized by the customer.

What if I have a question that is not answered here?

We are happy to answer any question you may have. Please reach out to your account Manager or account executive for assistance.