ATLASSIAN

Guide: GDPR Compliance

The Next Chapter

In the run-up to May 25, 2018, the day that the EU would start enforcing the General Data Protection Regulation (GDPR), many organizations were in a mad sprint to ensure they would be ready to comply with these new rules for the collection, usage, storage, and management of personal data.

Was this true for your org? If so, you were not alone.

Not surprisingly, despite the best intentions, reports suggest that many companies probably would not have passed an audit on May 26th. But even for teams whose personal data policies and practices are now in compliance with the GDPR, it's important to remember that this is not a one-and-done task.

In the last year, it's likely your organization took on new projects or programs that impacted its personal data-gathering practices. Likewise, your infrastructure will grow and evolve, and it will be critical to document your data collection and storage policies and operations. And as you hire new employees or individuals' roles change, you'll need to make sure everyone knows their responsibilities for protecting customer data.

We know that any compliance program is an ongoing effort. With the GDPR and other data privacy regulations looming on the horizon, we're committed to working with our community of customers and partners to help you secure personal data and maintain compliance.

Known fact: The financial consequences of GDPR can be severe

If there were questions about how strenuously the EU would enforce their new rules, those have now been answered. The financial consequences of failing to comply with the GDPR can be steep, as we've seen with recent fines. According to the law, penalties run up to €20 million, or 4% of worldwide annual revenue, whichever is greater.

This past January, Google was fined €56 million for failing to get informed consent from customers for the use of their personal data. It can be argued that Google attempted to get proper consent, though the language was spread out over multiple pages of content. It's apparent that, to regulators, it's more important to follow the spirit of the law – truly helping individuals understand how you're using their personal data – than technically complying with the letter of the law.

But it also appears that good-faith efforts count in the eyes of regulators. An unnamed German social media platform was fined for data breaches that exposed customer data, including passwords. But due to their prompt reporting and cooperation with regulating authorities, the penalty was only €20 thousand.

Main elements of the regulation

The intention of the GDPR is to acknowledge the value of personal data and the agency individuals have over their own personal data. Article 5 explains the spirit of the legislation:

1. Data should be processed with the fair consent of the data subject, transparently, and in accordance with the law.
2. Data will be collected and used for the purposes you give to the data subject, and not beyond this. (There are some exceptions, in the case of using data for the "common good.")
3. Only collect what you need, and no more. This benefits both the data subject and your organization; no sense in being responsible for protecting data you don't actually need.
4. Data should be maintained for accuracy, and when it is no longer accurate or up to date, steps should be taken to rectify this or delete the data.
5. Data should be kept in a form that identifies data subjects only for as long as is necessary and discards the data when it's no longer useful.
6. Data should be stored in a way that preserves its integrity and confidentiality.

Create a framework that builds trust across the organization

Beyond fines, there is another incentive to comply with the GDPR: demonstrating your organization's respect for personal data and building trust among your customers and partners. But IT organizations cannot do this on their own. This level of care for personal data requires participation and commitment from every arm of the company, and demands an organizational framework that guarantees everyone knows their roles and responsibilities.

Think of this as a people-process-documentation framework, the ultimate goal being to provide total transparency into the personal data you control and process internally and externally. Not only will you be able to prove compliance, but your product, sales, and marketing teams may also be able to leverage your personal data policies and procedures to build trust among the people you do business with.

The basic elements of this framework are:

Gather a cross-functional "Tiger Team"

Document policies, practices, and procedures

Audit to track changes for continuous improvement

Provide ongoing training so employees know their responsibilities

Build a team to spread the word and enforce policies

Before you assemble your Tiger Team, determine what types of personal data you need to collect in order to function as a business and deliver the best product or customer experience.

You'll want representatives from many parts of the organization, as it may not be obvious who collects personal data, for what purpose, and how they manage it, especially since some people may have access to third-party SaaS products that are invisible to the IT organization.

This probably goes without saying, but make sure your legal counsel is included in your Tiger Team. Not every organization has the same responsibilities, and you'll want to both make sure you're legally covered and that you aren't taking on more than you're required to do.

This team isn't necessarily responsible for actually writing policy; you probably don't want data security policies devised by a large committee. Instead, use this group to determine the breadth and depth of your organization's data collection and management requirements, and then appoint them to communicate the personal data management rules, policies, and processes to their respective teams.

Educate each team on their responsibilities

Each team member needs to understand the policies and procedures involved in obtaining consent to use personal data, as well as their responsibilities for storage and deletion.

Here's an example of a potentially challenging situation: Using a third-party tool, a product manager conducts a survey of potential customers, asking for personally identifying information so she can conduct follow-up interviews.

First, she should ensure that the contractual language addresses how the third-party vendor will protect, limit use of, and delete the customer data collected during the survey.

Second, the Product Manager should have a plan for disclosing to the survey participants what she intends to use the data for, and how long she intends to keep the data. She also needs to get consent to collect and use the data.

Finally, she should plan for how to store and securely dispose of the data once she no longer needs it.

Do I need a DPO?

Not everyone needs a dedicated Data Protection Officer (DPO). According to the UK's Information Commissioner's Office, you need a DPO if:

- Your organization is a public authority or body (except for courts acting in their judicial capacity).
- Your core activities require large-scale, regular, and systematic monitoring of individuals (for example, online behavior tracking).
- Your core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offenses.

Even if none of these situations apply to you, you may want a point-person charged with running your GDPR affairs. Just know that anyone who carries the title "DPO" is subject to very specific tasks, obligations, and responsibilities under the law. Make sure you document how you've decided to handle the leadership and coordination of your governance team to show that you're in compliance with the GDPR's principles of accountability.

Document your data collection, management policies, and procedures

In the event that you're audited for GDPR compliance, you will have to produce documentation that details what data you collect and how you manage it. You'll also want a written record of your policies and procedures in order to track tweaks and changes as your business evolves.

This documentation should be appropriate for the size and complexity of your organization. Don't make it so detailed that you're burdened by the upkeep, but do comprehensively record your data processing activities, and make sure your breach detection and notification plans are in place. As was the case with the German social media platform, even if you are audited and get dinged for an infraction, your documentation can show your good intentions, and your fine may not be as severe.

Some key elements to include in your documentation:

- **Personal data:** What personal data do you collect? How long will it be useful? When will you delete it?
- **Process analysis:** Know which processes involve personal data and why, and make sure you can justify the lawful use of this data.
- **Responding to data subject access requests:** Know how your organization will respond to data subjects' requests to view, port, or delete any or all of their data.
- **Communicating breaches:** Under the GDPR, you must report data breaches to regulators and notify anyone who may be affected. Work with your communications team to develop a crisis comms plan.
- **Information security management systems:** State which methodologies your org uses for testing security, noting any standards or best practices you follow, and any certifications you've received.

And if you're only recently subject to the GDPR and you're still developing your operations, consider documenting these plans in the form of a roadmap, complete with features and timelines, so everyone can see where you are and what's left to be done.

Audit for organization-wide compliance

Regardless of whether or not you are obliged to have a Data Protection Officer, you'll definitely want someone to lead the internal audits of your personal data management and security practices. How often you need to audit depends on how quickly your business changes, both in your practices and in personnel.

There are many ways to approach an audit. In general, you should:

- Audit for gap analysis between your current data protection and security practices and the GDPR rules.
- Get everyone who handles personal data to document what personal data they have, how it is used, where it is stored, and if and when it should be securely deleted.
- Request audit results and proof of compliance for all of your vendors who handle personal data to ensure they're following the rules of the data processor and have the proper security controls in place.
- Conduct a risk assessment to stay on top of your most vulnerable areas. And again, update this as your business changes.

Build awareness and offer ongoing training

Once your policies and procedures are in place, it's important that everyone in your organization is aware of their responsibilities for handling personal data and how to make sure the organization stays compliant.

Members of your "Tiger Team" can be charged with conducting regular training with existing and on-boarding personnel. Make sure they have access to up-to-date information that's specific to your organization's practices. They will also need to know how to respond if a data subject makes a request regarding their data, and, of course, how to handle the reporting of a breach or other infraction to the governing authorities.

And while vendors themselves are fully responsible for their own data handling standards and procedures, it's good practice to share information about your GDPR operations. This level of open communication and transparency can be vital your business in the event you have to work together through a personal data management infraction.

For more information and updates on our GDPR compliance practices, visit atlassian.com/gdpr.

Glossary of terms

- **Data Controller:** This is the natural or legal person, public authority, agency, or other body that determines the purposes for and means of processing personal data. An example: Google is the controller for the data associated with Gmail accounts.
- **Data Processor:** This is a natural or legal individual, public authority, agency, or other body that processes personal data on behalf of the Controller. An example: A cloud-based online survey tool processes personal data on behalf of its customers.
- **Data Subject:** Is a natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an ID number, location data, or an online identifier, or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **Subject Access Request:** Individual Data Subjects can make requests to access their personal data, either verbally or in writing. Generally, organizations have one month to respond to the request. Subjects can ask to see their data, port their data to another company, or delete their data in part or in full. They can also ask to have any mistakes corrected.