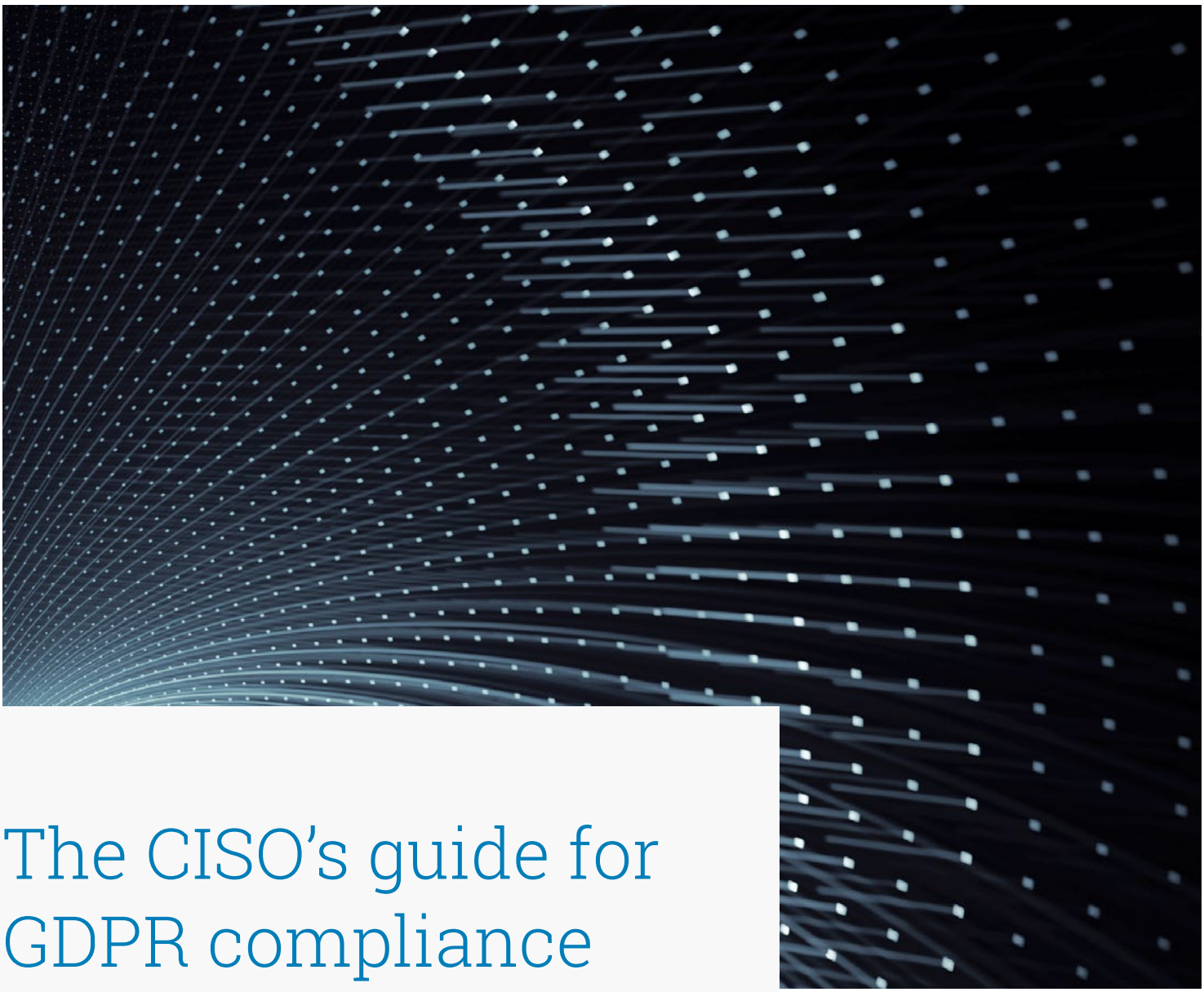
druva

White paper



The CISO's guide for GDPR compliance

Ensure proactive compliance monitoring with the cloud

Q221-20166

Executive summary

The European Union's General Data Protection Regulation (GDPR) went into effect in May of 2018 and has impacted organizations all over the world. For many, compliance has been a daunting and challenging task. In fact, GDPR regulators have imposed as much as €183M in fines for a wide range of infringements and data breaches[1].

The protection of EU citizen data has become a point of emphasis, and enterprises worldwide must ensure they have properly implemented GDPR-compliant data management practices. This white paper provides an overview of the GDPR, a deep dive into regulations particularly relevant to personal data protection and management, and how you can leverage the Druva Cloud Platform for GDPR compliance monitoring.

GDPR overview

The GDPR is a unified set of laws and regulations for data processing, and it includes severe penalties for noncompliance. GDPR compliance applies to any organization with a presence in the EU that processes personal data as part of its business activities or any organization outside the EU that offers goods or services to individuals in the EU.

The primary reasons for the GDPR regulation are:

- To provide EU citizens with more power over how their own personal data is used.
- To strengthen trust between digital services providers and the people they serve.
- To simplify the regulatory environment for international business operating in the EU.

> *By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today.*
>
> — Gartner[2]

GDPR categorization: controllers and processors

Determining your organization's exposure to GDPR as well as complying with it may be an overwhelming task, especially given the GDPR requirement of conciseness and clarity. The GDPR categorizes organizations into two roles: data controller and data processor. The GDPR defines[3] them as follows:

- A data controller is "the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing of personal data." They make decisions about and are responsible for any data processing activities.
- A data processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." They act on behalf of a controller and under their authority.

For example, an enterprise selling widgets online is a controller. The companies maintaining the website and shipping the product for that controller would be identified as processors. The enterprise/controller is the party responsible for GDPR compliance. However, if a shipper/processor fails to protect the customer's personal data, they may be subject to GDPR penalties as well.

Answering yes to any of the following questions, may point to your enterprise being a controller:

- Does my company offer goods or services that EU residents may receive either directly or indirectly (even for free)?
- Does my company monitor the behavior of EU residents (from inside or outside the EU)?
- Does my company have employees, or any other type of physical presence, in the EU (even a minimal one)?
- Do special/sectoral rules of an EU member state apply to your organization?

[1] CMS, GDPR Enforcement Tracker, 2020
[2] Smarter With Gartner "Gartner Predicts for the Future of Privacy 2020," 20 January 2020 https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020/
[3] EU GDPR, Article 4, Definitions

It's important to note that companies can be both controllers and processors. For example, a company may sell a SaaS storage solution, in which case they are a controller regarding their own sales activities and a processor regarding how they service their customer's data.

Personal data transparency

Organizations are expected to provide extensive information about the processing of its customers' personal data. To establish standard "purposes for processing" data, controllers must provide legal notice for processing data and legitimate reasoning for collecting personal data.

When transferring data outside of the EU (discussed below), the details regarding data protection in the recipient country, the mechanisms for transfer (for example, binding corporate rules, model clauses, or Privacy Shield), and how an individual can receive a copy of their personal data transfer policy, must be provided.

> *The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.*
>
> — EU GDPR[4]

Other requirements for notices include: the retention period for collected data, a statement of individual rights of access, transfer, data erasure (discussed below), information on supervisory authority and how to complain, and whether there is a contractual requirement to provide the data.

The notice must be provided at the time that the data is obtained, *when* and *if* the controller collects information directly from an individual. If the controller collects data indirectly, a notice must be provided within a month of when the data was collected.

To do list

- ✓ Review and update your Privacy Policy.
- ✓ For indirectly collected data, ensure notice is provided within 30 days from collection.
- ✓ Work with third parties collecting data on your behalf to ensure compliance.

Regulated personal data

The GDPR enforces a broad definition of personal data, referring to it as any information that could be used to identify an individual. This means that any piece of information regarding an individual (such as a phone number), even without any other identifying data, must be protected. This broad definition has an impact on mobile devices as well, as the regulation includes identifiers such as IP addresses or media access control (MAC) addresses. Explicit consent must be provided by the data collector in order to collect personal data. If not, this is a direct violation of GDPR regulation.

> *'Personal data' means any information ... such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*
>
> — EU GDPR[5]

[4] EU GDPR Recital 58, Transparency
[5] EU GDPR Article 4, Definitions

To do list

- ✓ Audit the data that you are processing and ensure you have GDPR-compliant grounds for processing.
- ✓ If you process genetic, biometric, or health data, ensure you follow individual member states' laws, as they often impose more stringent regulations.

Personal data breaches and notification requirements

The GDPR defines a personal data breach as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed." In the case of a personal data breach, the GDPR requires that:

- Processors notify data controllers promptly after discovery of a breach.
- Controllers must notify affected individuals and the supervisory authority within 72 hours.

> *The controller shall take appropriate measures to provide any information... relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.*
>
> — EU GDPR[6]

To do list

- ✓ Controllers should ensure that their third-party data processors are contractually obligated to promptly notify them of any data breaches.
- ✓ Data controllers and data processors should review and update their incident response plans and policies to ensure GDPR compliance.
- ✓ IT and IS teams should make sure that proper technical and organizational protections are in place to render data unintelligible in case of unauthorized access.

Data protection by design and accountability

Under the GDPR, proactive compliance monitoring is essential. Organizations must enhance security and privacy, and implement technical and organizational measures to show that they have integrated data compliance measures into their day-to-day data processing activities.

The GDPR recommends practices such as regular privacy impact assessments (PIAs), audits, policy reviews, activity records, and (in some cases) the appointment of a data protection officer (DPO). The GDPR requires the appointment of a DPO by companies that engage in regular and systematic monitoring of data subjects or that process sensitive data or criminal records on a large scale.

[6] EU GDPR Article 12, Transparent information, communication and modalities for the exercise of the rights of the data subject

The minimum requirements for most organizations to appoint a DPO include:

- The organization is a public body.
- Processing operations require large scale, regular and systematic monitoring.
- The organization has large-scale processing activities, especially with special categories of personal data.

To do list

✓ Ensure you have the proper budget and talent to comply with the GDPR — whether or not you are required to hire a DPO. Ensure that a full compliance program is in place for your organization, incorporating practices such as PIAs, audits, policy reviews, privacy, and security training.

✓ Review existing supplier arrangements and update the vendor questionnaires to reflect GDPR data processor obligations.

✓ Check that processes for GDPR-compliant record keeping of your organization's processing activities are in place.

Enhanced individual rights

At the heart of the GDPR is a strong focus on individual rights to privacy and control of personal data. Organizations are now required to provide individuals the following rights:

- ***Right to object personal data processing***

  Individuals have a right to object to the following types of processing: direct marketing, processing for research or statistical purposes, and processing based on legitimate interests or performance of a task in the public interest. Online services must offer automated methods for objecting and, if processing involves backup copies, destroying those backups.

> *"The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*
>
> — EU GDPR[7]

- ***Right to erasure***

  Individuals have the right to data erasure when their data is no longer necessary for the purpose for which it was initially collected, processed, or when data consent was withdrawn. The right also applies if data was unlawfully processed or collected. Additionally, if the personal data resides in a backup system (including legacy copies like tape backups), then all corresponding backup copies must be destroyed.

- ***Right to restrict data processing***

  The right to restrict processing of personal data applies to data accuracy disputes, objections to processing, or as an alternative to the right to erasure. If this right is exercised, the controller may only store the data. No further data processing is allowed unless explicit consent is given by the data subject. When it comes to automatic data processing, the restriction in data processing must be noted in the controller's IT systems by blocking the data, separating the data, or using any other technical means that would make the data temporarily unavailable. The right to restrict data processing also applies to situations where the controller doesn't have an immediate need to process the data but the data subject requires their personal data for eDiscovery and legal hold purposes.

[7] EU GDPR, Article 21, Right to object

- ***Right to access personal data***

  EU residents have a right to access their personal data, correct the data, and get a copy of the data in a commonly used electronic form (portability). The controller not only has to provide a data subject with a copy of their personal data undergoing processing, but the data provided must be portable — in that the data can be accessed via different applications and in cloud environments.

- ***Right to data portability***

  Data subjects have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format. They also have the right to transmit that data to another controller without hindrance from the initial controller.

- ***Right to rectification***

  The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing.

- ***Automated individual decision-making, including profiling***

  Individuals are provided the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them. These provisions restrict when organizations can carry out this type of processing and give individuals specific rights in those cases.

To do list

- ✓ Make sure your team is well trained regarding data portability, accessibility, and information requirements.
- ✓ Review your organization's ability to provide the necessary access to data.
- ✓ Think of your data storage solution with respect to handling processing restriction requests and legal hold requests.
- ✓ Implement processes for allowing data subjects to contact your organization to exercise the individual privacy rights mentioned above.
- ✓ Implement automated solutions that allow your organization to identify and remove information for data subjects, including backups.

Penalties and fines

When it comes to GDPR fines, there are two tiers: €10,000,000 or two percent of global revenue (whichever is higher) and €20,000,000 or four percent of global turnover (whichever is higher). The fines are discretionary and are imposed on a case-by-case basis.

> *Each supervisory authority shall ensure that the imposition of administrative fines … shall in each individual case be effective, proportionate and dissuasive.*
>
> — EU GDPR[8]

[8] EU GDPR Article 83, "General conditions for imposing administrative fines"

How Druva enables superior GDPR compliance monitoring

As the leading cloud data protection offering in the market, Druva focuses on how to solve compliance-related issues like the GDPR by leveraging the power of the Druva Cloud Platform. Here are some key points to keep in mind when it comes to leveraging Druva to meet your organization's GDPR compliance monitoring goals.

- ***Data visibility***

  To secure information and be compliant with GDPR, organizations must have visibility into where data lives. Druva gives organizations the ability to protect, collect, and monitor data on endpoints, servers, and cloud applications through a single monitoring dashboard. This broad data visibility provides organizations with an actionable understanding of their overall data and delivers real-time information on how best to deploy data security mechanisms to be compliant with the GDPR.

- ***Information governance***

  GDPR requires a holistic approach to protecting personal data and providing EU residents with access to that data. Traditional data governance has focused on forcing data centralization, which only provides visibility into information that is stored centrally. With the decentralization of data creation on mobile devices and cloud apps, organizations need to take a different approach to govern that data as part of developing an effective data governance process. Druva leverages the cloud to allow organizations to easily centralize data source policy management and enforcement to bring in decentralized data under the control of GDPR compliance.

- ***Continuous compliance monitoring***

  GDPR requires data processors and controllers to monitor the content, location, and use of EU resident information no matter where it lives. With Druva, organizations can automate the process of proactively monitoring information for compliance violations whether that data is on a traditional endpoint or in a cloud application.

- ***Secure data transfer***

  With GDPR, security must move with the data no matter where it resides. Druva uses industry-leading standards based on TLS 1.2 and AES 256 encryption with unique keys for each customer as well as simplified and integration key management. Druva can also prevent data from leaving the EU in the event that organizations have not yet established acceptable transfer mechanisms.

- ***Right to data erasure***

  One of the major challenges facing organizations dealing with the GDPR is how to erase information at the request of data subjects in order to purge all data, including backups, and prevent any subsequent processing. According to the GDPR, consent is not permanently binding, and there must be a possibility to withdraw it. While there are some caveats with this provision of GDPR, any lawful requests of data erasure must be processed in a timely manner. Druva provides compliance capabilities, via Druva inSync, that enables customers to delete files and emails in source and/or backup snapshots — with some limitations (e.g., cannot delete files for legal hold or preserved users, tablets/smart phones, etc). This capability can be applied to emails or files detected either via proactive compliance or metadata search. These features can be harnessed to address data erasure requests.

To further help guide enterprises through the various GDPR requirements, Druva has mapped every GDPR article against Druva's obligations as the data processor and its customers' obligations as data controllers. Please review the Druva GDPR Shared Responsibility Model document and visit the Druva Data Privacy Law and Regulation Compliance page.

Takeaway — GDPR is all about data management and compliance monitoring

GDPR is not just about protecting individual data, it's also about knowing where all your data resides. It is critical that organizations manage the full visibility, access, control, and ultimately erasure of all personal data for EU citizens. When it comes to fines and punitive damages, the GDPR does not discriminate between traditional client/server infrastructure versus modern compute capabilities such as cloud applications and mobile devices. Therefore, not knowing where data resides is no excuse, and it may result in a direct violation. Any technology solution that attempts to enable GDPR compliance must focus on being able to see all data, classify all data, and secure all data.

Enable GDPR compliance and ensure your data is always on, always safe.
Visit druva.com/solutions/proactive-compliance/

druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.