



 White Paper

THE GDPR COMPLIANCE GUIDE FOR BUSINESS

The Next Generation of EU Cloud Data Protection

Executive Summary

The next generation of data protection requirements has arrived for the European Union (EU) in the form of the General Data Protection Regulation (GDPR). The regulation, which goes into effect on May 25, 2018, will have an impact on organizations all over the world and has sent them scrambling to get a handle on what the GDPR is, what it means to their organization, and how they are going to achieve compliance. For many, this is a daunting task and, despite best efforts, by the end of 2018 over 50% of companies affected by the GDPR will not be in full compliance with its requirements, according to a March Gartner Research report, *Focus on Five High-Priority Changes to Tackle the EU GDPR*.

When examining the GDPR compared to its predecessor, the EU Data Protection Directive (DPD), there are some stark differences. While the DPD was more of a suggestion when it came to the protection of EU citizen data, the GDPR comes out of the box with teeth, in the form of audits and financial penalties for non-compliance. To say that protection of EU citizen data, no matter where it lives, “just got real” would be an understatement.

Companies must first determine what personal data the organization collects, confirm where that data is stored and then clarify for what purpose it is used. This white paper will provide organizations with an understanding of the GDPR, a deeper look at the relevant portions of the regulations, and a roadmap for how processes and technologies can be used to enable and maintain compliance.

“Global companies operating in the EU or processing personal data collected in the EU need a roadmap to comply with the new GDPR requirements.”

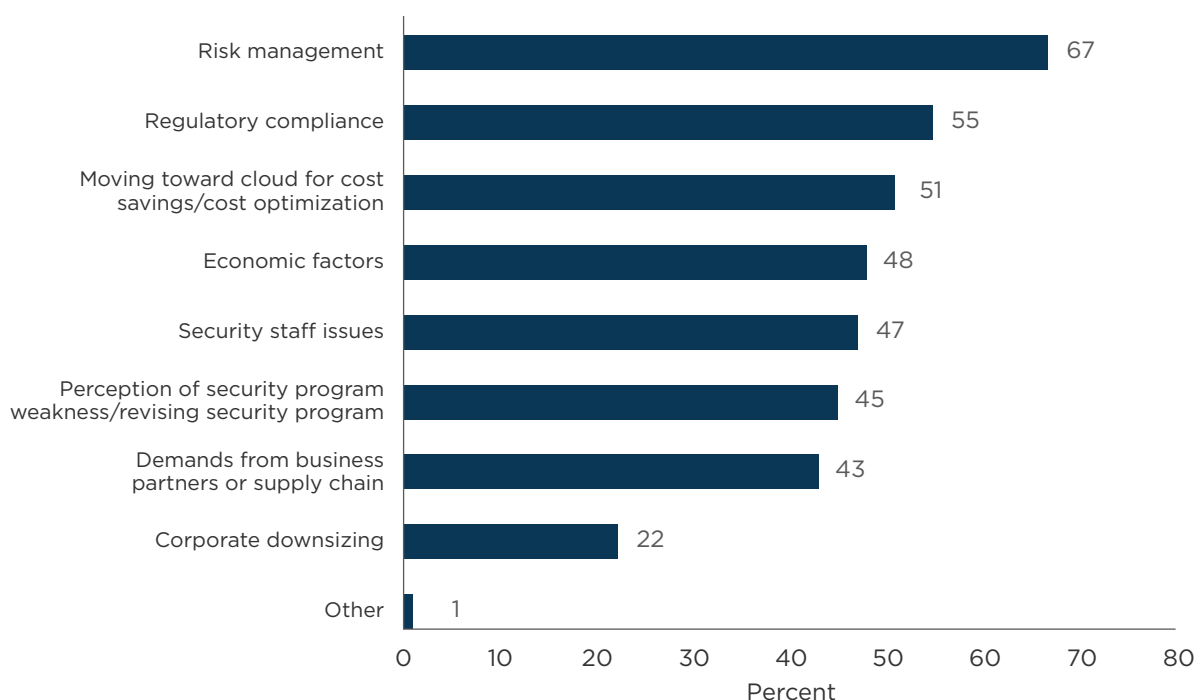
—451 Research—GDPR set to make personal data, privacy protection uniform across EU

GDPR Overview

Companies have little time to prepare for some drastic changes in the way they will need to handle the personal data of EU citizens. The GDPR creates a unified set of laws and stricter regulations for data processing, and it also specifies steep penalties for noncompliance. These penalties are in the form of administrative fines and can be imposed for any type of GDPR violation, including those that are purely procedural. Companies across the globe are already preparing for the change and have allocated budgets accordingly.

The results of Gartner's 2016 Security Buying Behavior survey show that privacy concerns and having experienced a breach are the leading influencers when determining security budgets.

Risks Influencing Security Spending by Region



The primary reasons for the new regulation are:

1. To provide EU citizens with more power over how their own personal data is used
2. To strengthen trust between digital services providers and the people they serve
3. To provide businesses with more clarity for operating across the EU single market

The GDPR vs. the DPD

The reach of the GDPR is significantly larger than that of the DPD. Under the DPD, organizations had to comply with the EU rules only if they used equipment in the EU to process or collect personal data. Such equipment included the use of cookies and requesting users fill out forms.

The GDPR will apply to any organization with a presence in the EU that processes personal data as part of its business activities. Even a minimal presence will suffice. Factors such as having a local representative working in the EU or having an office, bank account, or even a postal office in the EU could potentially mean the GDPR would apply.

The business activities subject to the GDPR include any advertising, marketing, or services catering to EU residents. Even if an organization is not deemed to have a presence in the EU, offering of goods and services to the EU residents or monitoring their behavior would be subject to the GDPR. Monitoring is defined as any tracking of individuals online to create profiles and/or analyze or predict personal preferences, patterns of behavior, or attitudes. While mere accessibility of a site from within the EU is not sufficient, the use of an EU language/currency, or an ability to place orders in that other language will be relevant.

Unlike the DPD, which was primarily a recommendation/best practice guidance for the individual member states' privacy laws, the GDPR is an actual enforceable regulation. However, the GDPR does allow member states to legislate on data protection when it comes to public interest tasks or is carried out by a body with official authority. Other GDPR provisions may be further restricted by member state laws.

Your Role Under the GDPR

The GDPR affects organizations based outside the EU offering goods and services (even for free), that process or monitor EU citizens' data. Determining your organization's exposure to this regulation as well as providing all the required information may be an overwhelming task, especially given the GDPR requirement of conciseness and clarity. Ensure that you first answer certain key questions in order to determine whether your organization is just an EU "data controller" or bound to comply in some other respect, under the GDPR.

Answering yes to any of these, in part or in whole, is the first sign that your organization needs to prepare for GDPR compliance.

Is Your Company a Controller or a Processor?

Initial Questions To Answer:

- ☒ Does my company offer goods or services to EU residents (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 apply to your organization?*




Transparency (i.e. Privacy Policy)

According to the GDPR, having a page-long standard privacy notice/policy will no longer work in the EU. Organizations are expected to provide extensive information about the processing of their personal data. In addition to the identity and contact details of the controller, companies must provide contact details of the data protection officer. In addition to standard “purposes for processing,” controllers must include the legal basis for processing and the legitimate interest pursued by the controller.

Data transfers outside the EU must include details regarding the data protection in the recipient country, mechanisms for transfer (i.e. Binding Corporate Rules, Model Clauses, or Privacy Shield), and how an individual can get a copy of the applicable transfer policy or document. Some other requirements for notices include: retention period for data, statement of individual rights of access, port, and erasure (discussed below), information on supervisory authority and how to complain, and whether there is a statutory or contractual requirement to provide the data. The notice must be provided at the time the data is obtained, if the controller collects information directly from the individual. If the controller doesn't collect information directly, a notice must be provided within a month of collection or when the first communication with the data subject is made.

*Review the laws of individual EU member states to ensure compliance

Transparency — Your Organization's 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 Data



The definitions of Sensitive Data and Personal Data have been expanded by the GDPR. Under the DPD, each of the 28 member states developed their own interpretation of what constituted Personal Data. The GDPR, in contrast, enforces a strict and broad definition of Personal Data, referring to any information that could be used, on its own or in conjunction with other data, 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, will need to be protected. This broadened definition has a profound impact with regards to mobile devices as well, as the regulation includes identifiers such as IP addresses or media access control (MAC) addresses. And if explicit consent to the collector was not given, or if the person was not informed that the collection was taking place, then current market observers will find that this is in violation of the regulation.

“Personal data could include profiles for marketing purposes, email addresses, phone numbers, or a host of other data that might have been purchased, transferred from another company, or gathered directly during a business transaction or use of a service.”

—Gartner—“New GDPR Mandates Require Changes to Storage Management Strategies for All Global Enterprises”

In addition to racial and ethnic origin, political opinions, religious and philosophical beliefs, trade union memberships, health information, sexual orientation, and sex life, genetic data and biometric data have been added to the sensitive data list. The grounds for processing sensitive data under the GDPR broadly replicate those of the DPD.

Regulated Data — Your Organization's To Do List:

-  Audit the data that you are processing and ensure you comply with the grounds for processing requirements
-  If you process genetic, biometric or health data, ensure you follow individual member states' laws, as they have a broad right to impose further 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.” The GDPR requires controllers and processors to follow four notification requirements.

Notification Requirements:

1. Notify data controllers *“without undue delay”* after discovery of the breach.
2. Notify the supervisory authority *without undue delay* and, where feasible, *no later than 72 hours* after becoming aware of it.
3. Notify the affected data subjects *without undue delay, no later than 72 hours* after becoming aware of it.
4. Maintain an internal breach register.

To Do List for Your Organization

-  Data controllers and data processors should review and update their incident response plans and policies to ensure compliance with the GDPR

-  IT and IS teams should make sure that proper technical and organizational protections are in place to render the data unintelligible in case of unauthorized access
-  Customers should ensure that their third-party data processors notify them of any data breaches via contractual commitments

Data Protection by Design and Accountability


Under the GDPR, companies are required to actively monitor their data processing activities, which means enhanced security and privacy by design. Organizations must implement technical and organizational measures to show that they have integrated data compliance measures into their day-to-day data processing activities.


Practices such as regular Privacy Impact Assessments (PIAs), audits, policy reviews, activity records, and (in some cases) appointment of a data protection officer (DPO) are not only recommended, but are prescribed by the new regulatory regime. DPO appointment is required for companies that engage in regular and systematic monitoring of data subjects or process Sensitive Data or criminal records on a large scale. While there is an exemption for the above requirement for companies with fewer than 250 employees, the exemption will not apply where Sensitive Data is processed, which in many cases will nullify the usefulness of the exemption.

Minimum requirements for many organizations to appoint a DPO include:

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

To Do List for Your Organization

-  Make sure you have the proper budget and talent to comply with the GDPR—whether or not you are required to hire a DPO, compliance with the new requirements will require expertise and resources

-  Ensure that a full compliance program is designed for your organization, incorporating practices such as PIAs, audits, policy reviews, privacy, and security trainings
-  Review the existing supplier arrangements and update the vendor questionnaires to reflect the GDPR data processor obligations
-  Implement processes for GDPR-compliant record keeping of your organization's processing activities

Enhanced 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 disclose the intended use and duration of storage of the data acquired and allow EU citizens to control the use, storage, and management of their personal data.



Right to object

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 an automated method for objecting and, if processing involves backup copies, then the automation of destroying those backups would provide the needed scalability.



Right to be forgotten

Individuals have a right to erasure (also referred to as a **“right to be forgotten”**). The right applies when data is no longer necessary for the purpose for which it was initially collected, processed, or when the consent of the data subject was withdrawn. The right also applies when the data was unlawfully processed or collected (not in accordance with the GDPR). If the personal data resides in a backup system, then all corresponding backup copies would have to be destroyed in order to comply. Legacy copies, like tape backups, would have to be recalled and erased, making the task of identifying data and processing these types of requests nearly impossible in certain circumstances.

“Automation of data backup exercises for only the information they are required to backup will be necessary. And automated purging of the nonrequired content is another function organizations will be seeking once the law goes into effect, if not sooner.”

–Gartner—EU Privacy



Right to restrict processing

The DPD’s right to “block” is replaced with a **right to restrict processing** of their data. This right applies to data accuracy disputes, objections to processing, or, when used as an alternative, to the right to erasure. If this right is exercised, the controller may only store the data. No further processing is allowed absent an explicit consent of the data subject or for a limited number of purposes (i.e. protection of individual rights of another person/important public interest). When it comes to automatic processing, the restriction 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 processing will also apply to situations where the controller doesn’t have an immediate need to process the data but the data subject requires the personal data for litigation purposes, which may mean that controllers must retain data storage solutions for former customers.



Right to access the data

Finally, EU residents now have a **right to access the 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 the personal data undergoing processing, but the data provided must be

portable. The data portability requirement means that the controller must provide information in a structured, commonly used and machine readable form.

To Do List for Your Organization





- ☒ Make sure your team is well trained on the GDPR requirements regarding the 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 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.

Transfers of Personal Data

Transfers of personal data outside of the the European Economic Area (EEA) are regulated by the GDPR in a similar manner to the DPD. The Commission will determine which countries are "adequate" for data transfers and which countries need additional transfer mechanisms (such as the Model Clauses, Binding Corporate Rules, or Privacy Shield). The list of adequate countries is still the same, and United States companies have a choice of either using Binding Corporate Rules for intracompany data transfers, Model Clauses, or certification under the Privacy Shield.

What has changed are the penalties. Companies that fail to comply with the GDPR's data transfer rules may be penalized with fines equivalent to up to 4% of worldwide annual turnover.

To Do List for Your Organization

-  Review and assess your current data transfer mechanisms
-  Discuss whether or not to obtain a Privacy Shield certification
-  Consider whether Binding Corporate Rules (BCRs) would be an appropriate mechanism for intracompany data transfers
-  Make sure the vendors handling your company's data have appropriate data transfer mechanisms in place

Penalties and Fines

The stakes are much higher with the GDPR than they were with the DPD. The administrative fines imposed by the supervisory authorities are much more significant and may be imposed for any type of violation of the GDPR, including purely procedural infringements. There are two tiers of fines: 10,000,000 Euros or 2% of global turnover, whichever is higher, and 20,000,000 Euros or 4% of global turnover, whichever is higher. The fines are discretionary and are imposed on a case by case basis. For example, the loss of a single managed mobile device that contains personal data constitutes a breach that could result in a €20 million fine.

“The costs of remedying noncompliance are staggering—in the millions of dollars. But the costs pale compared with the potential loss businesses can suffer from consumer distrust created by exercising the wrongful acquisition or misuse of personal data.”

—451 Research—“GDPR set to make personal data, privacy protection uniform across EU”

Druva Enables GDPR Compliance

As only the cloud-native data protection SaaS offering in the market, Druva spends a lot of time thinking about how to solve compliance-related issues like the GDPR by leveraging the power of the public cloud. Here are some key points to keep in mind when it comes to leveraging Druva Cloud Services to meet your organization's GDPR compliance goals.



Data Visibility

To secure information and be compliant with GDPR, organizations have to have visibility into where data lives. Druva gives organizations the ability to protect, collect, and monitor data on endpoints, servers, and cloud applications across the global enterprise. This broad visibility provides organizations with an actionable understanding of their overall data-attack surface and delivers real-time information on how best to deploy 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 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 device and cloud apps, organizations need to take a different approach to govern that data as part of developing an effective 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 Data 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 the Transfer

With GDPR, security must move with the data no matter where it resides. The Druva Cloud utilizes 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 be Forgotten (a.k.a. Right to 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 erasure have to be processed in a timely manner. Druva provides defensible deletion capabilities to be able to comply with erasure requests, including a robust audit trail to definitively demonstrate that the information was deleted.

The Big Takeaways

1

GDPR is Coming Fast

The GDPR is a reality and well on its way to impacting organizations of various sizes around the globe. While many may look at the GDPR as a means to procure and implementation additional security mechanisms in their environments, they would be missing the point.

2

GDPR is All About the Data

Not just protecting data, but actually knowing where all your organizational data resides. It will be critical that organizations manage the full visibility, access, control, and ultimately erasure of all personal information 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 will no longer be a valid excuse, in fact, 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.

3

The Penalties Are Real

The stakes are much higher with the GDPR, compared to the less enforceable DPD. The GDPR comes out of the box with real teeth — audits and financial penalties for non-compliance. The administrative fines are much more significant and may be imposed for any type of violation, including purely procedural infringements.

About Druva

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at <http://www.druva.com> and join the conversation at twitter.com/druvainc.



Druva, Inc.

Americas: +1 888-248-4976
Europe: +44 (0) 203-750-9440
APJ: +919886120215
sales@druva.com
www.druva.com