Where There Are Challenges, There Are Opportunities

Global opportunities for VARs, ISVs, and MSPs surrounding GDPR compliance

WWW.INGRAMMICROCLOUD.COM

Contents

Overview

The General Data Protection Regulation (GDPR) has been making waves around the world — and for good reason. While the regulation is only intended to protect the personal data of European Union (EU) residents, due to the global nature of how and where individuals' personal data is stored, and the fact that many companies holding that personal data are also holding the personal data of non-EU residents, it has become the de facto global mandate.

In effect since May 25, 2018, GDPR applies to anyone collecting or processing personal data from a data subject who resides in the EU. The processor or collector could be located anywhere in the world. U.S. companies selling anything to EU residents or even having EU resident web traffic will have to comply if they want to continue to access the EU market.

It is not the intention of this paper to detail the specifics of GDPR and GDPR compliance, but instead to stress the regulation's importance for technology partners — both in terms of their own compliance, and in terms of the tremendous opportunity for partners to provide GDPR guidance and solutions to their customers.

GDPR and Technology: A Match Made in the Cloud

"The new regulations provide unique opportunity for customers to work closely with their technology and services providers to modernize their infrastructure, governance, and data management tools and leverage GDPR as a catalyst for IT and business modernization." – Andrew Smith, senior research analyst, Storage Software.

Cloud computing and GDPR are inexorably intertwined. The rise of the digital economy creates an urgent need to account for and secure the vast amounts of information and data being generated around the world. Due in large part to the widespread growing use of cloud solutions, personal data is easy and inexpensive to collect and store — and much of that collection and storage is unregulated and unprotected.

Just as the cloud created the need for GDPR, cloud is the leading technology to facilitate compliance with GDPR. Cloud can help boost GDPR compliance, as moving data to the cloud speeds and simplifies the tasks of upgrading security practices and data protection standards to meet the new regulations. In advance of the regulation's effective date, most major technology vendors — including AWS and Microsoft Azure, committed to ensuring GDPR compliance to support their customers operating in the EU. Similarly, publishers of cloud-based solutions are rushing to incorporate and promote GDPR compliance not just for their solutions, but also for their policies, processes, and procedures. And, perhaps inevitably, entire new applications and services — including data governance and management, security, and user consent tools are entering the market in an effort to capitalize on the wide-reaching regulation.

By storing data in sophisticated cloud environments, organizations are able to centralize data from all assets in one location, rather than having several data access points. This is important for improving the visibility, accessibility, and auditability of the data. In addition, cloud storage solutions can offer operational benefits including the automated backups and the prevention of data leakage.

Cloud technology is both the precipitator and ultimately the solution to what is certain to be an ever-increasing concern with the safety and confidentiality of the vast quantities of data that define our digital economy.

Summary of GDPR Compliance

In the full text of GDPR there are 99 articles setting out the rights of individuals and obligations placed on organizations covered by the regulation. While a full discussion of the articles and considerations of GDPR are outside the scope of this paper, it is useful to outline the main compliance points in the regulation to highlight the rights, responsibilities, and data touchpoints affecting partners and their customers.

1. **Explicit consent**
   Companies must obtain explicit consent to collect sensitive personal data. Terms of consent must be clear and easy to understand — and consent must be easy to give and easy to revoke. Once collected, this consent must be documented, and the data subject is allowed to withdraw his consent at any time.

2. **Lawful, fair and transparent processing**
   The companies that process personal data must process the personal data in a lawful, fair and transparent manner. Essentially this means that companies must be collecting the personal data for a legitimate purpose and must fully inform data subjects about their processing activities.

3. **Timely breach notification**
   Controllers have 72 hours to report a data breach to both the data subjects and the relevant supervisory authorities. Failure to report breaches within this timeframe may lead to fines.

4. **Right to access data**
   Users have the right to request their existing personal data profile, and companies must be able to provide them with a fully detailed and free electronic copy (in a common format) of the personal data collected about them. This report must also include the various ways the personal data is being used. Users also have the right to require a business to correct errors in their personal data held by the business.

5. **Right to be forgotten**
   Also known as the right to data deletion, once the original purpose or use of the personal data has been realized, data subjects have the right to request that their personal data be fully erased.

6. Data portability

GDPR gives data subjects rights to their own personal data. They must be able to obtain their personal data from a company and reuse that same personal data in other ways of their choosing.

7. Privacy by design

This section of GDPR requires companies to design their systems with the proper data protection protocols in place from the start.

8. Data transfers

Controllers must ensure that personal data is protected and GDPR requirements respected, even if processing is being done by a third party. This means controllers have the obligation to ensure the protection and privacy of personal data when that data is being transferred outside the company, to a third party, or other entity within the same company.

9. Limitation of purpose, data and storage

Companies are expected to limit the processing, collect only that personal data which is necessary, and not keep personal data once the processing purpose is completed.

10. Awareness and training

Organizations must create awareness among employees about key GDPR requirements and conduct regular trainings to ensure that employees remain aware of their responsibilities with regard to the protection of personal data and identification of personal data breaches.

A Word About Fines

Fines for non-compliance with GDPR can be up to 4 percent of a company's global revenue or 20 million euro, whichever is greater.

Not Just Electronic Data

Even in our increasing digital age, companies still retain paper records that may be subject to GDPR. It is wise to justify this data's retention along with a plan to store it securely — or destroy it.

Data Subjects' Rights Under GDPR

- Right to view and understand processing of their personal data
- Right to restrict or object to processing of personal data
- Right to rectification of inaccurate personal data
- Right to erasure of personal data
- Right to receive their personal data

Challenges Customers Face

GDPR is fundamentally changing the way in which personal data is handled across every business sector, from healthcare to banking and beyond. With eleven chapters and 99 articles, many companies will find it difficult to sift through the text of the GDPR to identify what parts of the regulation apply to them, determine what steps to take to move into compliance, and decide which technology tools and/or service providers may help with that compliance.

To meet GDPR requirements, companies will first need to answer some difficult questions:

1. What personal data do we have?
2. Where is the personal data stored?
3. How and when did we obtain the personal data?
4. What is the business purpose for this personal data?
5. Is the personal data accurate
6. Who has access to the personal data?
7. Do we have permission to use the personal data? For what purpose? Or is there another legal justification for the processing of the personal data?
8. How is the personal data secured?
9. Are we sharing this personal data with other entities, internal or external?
10. How long do we need to retain this personal data?

Next, companies need to put the building blocks in place to achieve compliance. Some of the more difficult components of the mandate include:

Data Storage and Access

Businesses need to assess where personal data is stored and who has access to personal data. They will need to audit all data sources to see what personal data is collected, how it is used, who can use it, and for how long. Companies will need the ability to provide personal data to a user upon request, or delete all personal data being held, which can be a challenge when personal data is held in multiple applications on multiple servers.

Security

Companies will need to implement best practices surrounding data collection and storage in areas such as encryption, data anonymization or pseudonymization, and identity and access management. Under GDPR, companies must prove that any third-party holders of personal data have implemented appropriate technical and organizational controls. Given the potential for large amounts of personal data to be involved, this implies that companies may need to introduce considerable automation, and/or have systems that enable them to quickly recall personal data from third-party control.

Usage and Movement

GDPR requires businesses to keep a record of processing activities that use personal data. One of the more challenging parts of the regulation are “data subject rights” stipulating that upon request, companies must provide details such as the purpose of the processing, categories of personal data involved, all recipients of the personal data, and more.

A Currency of Trust: Opportunities for VARs, SPs, and ISVs to Capitalize on GDPR

"Clients will be relying on their providers to help them meet regulations, which is a great opportunity to build on your relationships, all while creating new business with current and potential end users."[2] – IT trade association CompTIA

➔ **Fast Fact: 68% of U.S.-based companies expect to spend $1 million to $10 million to meet GDPR requirements.**[5]

The business challenges that result from GDPR compliance represent an opportunity for IT value added resellers (VARs), service providers (SPs), and independent software vendors (ISVs). These firms are in an excellent position to deliver consultative advice, technology building blocks, cloud services, design and implementation direction, employee training, and other kinds of value to customers who are working toward GDPR compliance.

Technology is only part of the solution; it is as much about improving processes, which takes the help of skilled and trained professionals. GDPR provides an enormous opportunity for VARs, SPs, and ISVs to guide their customers through the potentially complex regulation while offering a new set of revenue-boosting services. Partners can use GDPR to strengthen their relationships with existing customers and create new business with prospects seeking to grow their compliance.

How significant is the opportunity? The U.S. GDPR market alone generated $416 million in 2017, and the market is forecast to grow to $537 million in 2022. That equates to a compound annual growth rate (CAGR) of 5.2% for the 2017–2022 period.[1] Simply put — the opportunities for partners surrounding GDPR are enormous.

➔ **Fast Fact: The U.S. GDPR market is forecast to hit $537 million in 2022.**[1]

Opportunities for VARs

According to a recent Netskope Cloud Report, EU firms are unaware of how many cloud applications their organizations are actually using, which on average is believed to be over 600 software programs.[3] Symantec puts that number at closer to 1,000 when considering firms worldwide.[4]

Starting with that level of uncertainty, VARs can easily make the case that it will be beneficial for companies to have a single trusted technology provider for all of their cloud-based applications. VARs may even choose to incorporate GDPR compliance services as an explicit part of their business model.

Opportunities for SPs

One of the biggest implications of GDPR is the requirement for accurate storage, visibility, and monitoring of personal data. Organizations that have traditionally relied on legacy on-premise IT infrastructure are finding that they are unable to enact the strict monitoring nor the stringent security assurances required by GDPR and will be looking to service providers to provide the infrastructure, security, and data management tools necessary to achieve compliance.

Opportunities for ISVs

GDPR is creating opportunities for ISVs as well. The regulation includes "Privacy by Design," which requires data protection to be included within a system's design, rather than something that is added later. ISVs who design their solutions with security built right in will have a distinct advantage. In addition, customers will be looking for assistance with solutions that help them track and report consent, respond to EU resident requests for how their data is used or for data erasure, and other rights they have under GDPR. ISVs that offer solutions to these challenges will be able to capitalize on the opportunities provided by GDPR.

Fast Fact: Processor or Controller?

Does the organization determine the purpose of the data processing? (The Why?)

Does the organization determine the means of the data processing? (The Hows?)

Yes = Controller
No = Processor

Note: It is possible for an organization to be BOTH a controller and a processor.

GDPR Compliance Technology Tools

Companies will need to increase automation and streamline their operations in order to meet the challenge of sustaining GDPR compliance over the long term. As a business's data portfolio continues to grow and become more complex, it is difficult to conceive of GDPR compliance being possible without an automated approach to compliance. Automation will also prove more cost-effective and will greatly simplify production of the reports and audit logs needed to prove compliance.

Key components will include use of state-of-the-art data protection technology, continuing investment in cybersecurity, improvements to internal processes, and additional automation elements. A few of the categories of available technology tools that will prove useful are:

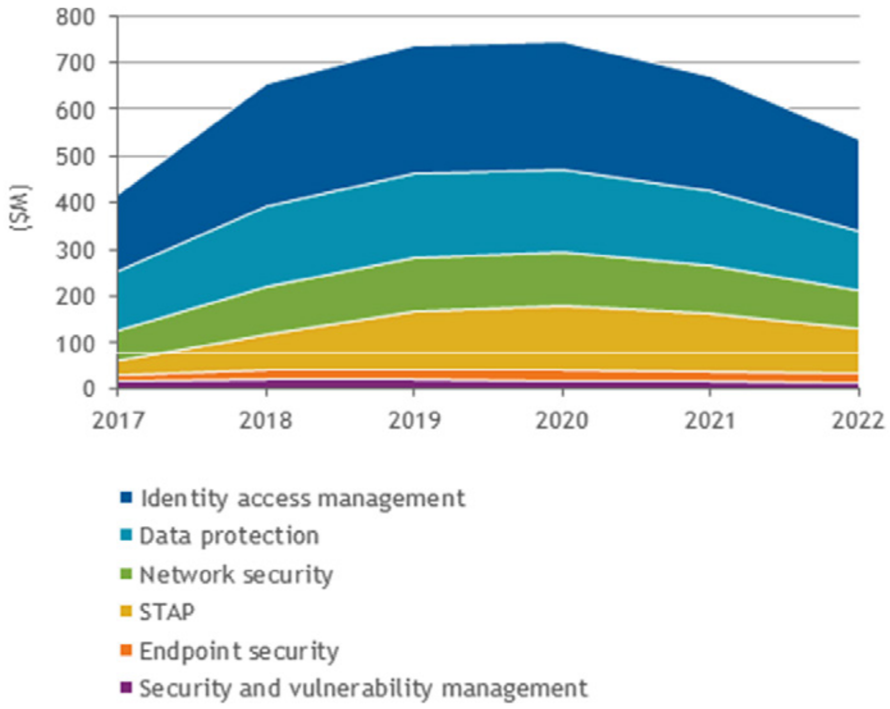
1. **Backup and Disaster Recovery**
   Backup and recovery solutions are a necessity for all companies, but robust tools that support data encryption and can combine physical, virtual, and cloud backup options will be an integral part of companies' GDPR compliance.
2. **Business Applications**
   Business applications including ERP, accounting, and productivity tools can support GDPR compliance with features including role, record, and field-level security and in-transit encryption.
3. **Cloud Enablement Services**
   Cloud enablement services help partners and their customers move their businesses to the cloud, where a comprehensive GDPR compliance platform is easier to deploy, monitor, and manage.
4. **Communication and Collaboration**
   Technology tools including collaboration platforms that provide data storage capabilities can help companies comply with various mandates in the regulation, by tracking the data used, recipients, and data flow.
5. **Digital Marketing**
   The digital marketing tools companies leverage must be carefully vetted to ensure that they are collecting, storing, processing, and sharing data in compliance with GDPR.
6. **Infrastructure**
   Many infrastructure solutions, including AWS and Azure, are leaders in GDPR compliance in large part because their businesses models required early and robust adherence to the regulations.

7. Data Protection and Security

Not surprisingly, network and endpoint security solutions are of fundamental importance to any GDPR compliance model. A growing security segment is the Cloud Access Security Broker (CASB). CASBs consolidate multiple types of security policy enforcement, such as authentication, device profiling, encryption, tokenization, alerting and malware detection/prevention.

IDC predicts that U.S. GDPR spending by segment will be dominated by identity access management, data protection, and network security solutions.[1]

U.S. GDPR Security Products Spending by Segment, 2017–2022



Source: IDC 2018

How Ingram Micro Cloud Can Help

To capitalize on the opportunity presented by GDPR, VARs, SPs, and ISVs must:

1. Educate themselves with enough knowledge of GDPR to position their firms as trusted experts on compliance.

2. Educate customers about the impact of GDPR and the steps they must take to obtain and retain compliance.

3. Become familiar with and supply the cloud solutions that will help customers with their compliance needs.

Ingram Micro Cloud helps streamline compliance by offering a comprehensive portfolio of cloud solutions, a billing and provisioning platform, educational materials, and support designed to help partners and their customers understand the impacts of GDPR and gain compliance.

VARs and SPs can deepen their customer relationships by offering end-to-end GDPR support services. Using Ingram Micro Cloud's streamlined, automated billing and invoicing, resellers can scale their compliance offerings profitably without increasing overhead. By partnering with a cloud services distributor like Ingram Micro Cloud, VARs and SPs can continue to offer the latest solutions, without the large capital expense of maintaining their own infrastructure or negotiating terms and contracts with individual vendors. It adds up to more possibilities and more opportunities.

Using tools available through Ingram Micro, ISVs can supply their cloud solutions using world-class secure and compliant delivery platforms ranging from simple to fully customizable, with automated orders, billing, payments, configuration, provisioning, management, and more.

Conclusion

Moving forward, the GDPR will be an intrinsic part of the global digital economy. It is increasingly likely that other countries will join the EU in implementing common sense data protections. The uncertainty surrounding the details of the regulation and the technology and services required to navigate compliance present significant opportunities to VARs, SPs, and ISVs. Ingram Micro Cloud provides partners with access to the cloud-based tools, information, and services needed to grow their own firm's GDPR compliance, and to add and grow a lucrative new compliance practice to their operations.

Disclaimer

GDPR compliance is a complex topic and this paper is not intended to serve as a compliance guide. We encourage you and your customers to seek professional advice specific to your situations.

Sources

1. IDC, U.S. GDPR Security Products Forecast, 2018–2022: Impact of GDPR on Spending *https://www.idc.com/getdoc.jsp?containerId=US44150418*
2. CompTIA, New EU Data Protection Regulations – What Can the Channel Do to be Ready? *https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2016/06/28/new-eu-data-protection-regulations-what-can-the-channel-do-to-be-ready-*
3. Netskope Cloud Report 2017
https://resources.netskope.com/cloud-reports/september-2017-netskope-cloud-report
4. ETCIO.com
https://cio.economictimes.indiatimes.com/news/strategy-and-management/enterprises-on-average-use-up-to-1000-cloud-apps-but-their-cios-think-its-just-30-or-40-apps/58410934
5. PwC, Pulse Survey: US Companies ramping up GDPR budgets
https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf
6. European Commission, 2018 reform of EU data protection rules
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
7. EUGDPR.org
https://eugdpr.org/
8. Deloitte, GDPR and the impact on cloud computing
https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html
9. Compare Cloud, Cloud Holds the Key to GDPR Compliance — but not without a culture shift
https://www.comparethecloud.net/articles/cloud-holds-the-key-to-gdpr-compliance-but-not-without-a-culture-shift/

INGRAM MICRO®

About Ingram Micro Cloud

At Ingram Micro Cloud, we view cloud not just as a single technology, but as a foundational platform to run and drive a whole new way of doing business. We help resellers and partners get up and running with cloud quickly, enabling them to transform their business. We help our clients monetize and manage the entire lifecycle of cloud services, infrastructure and IoT subscriptions, helping them simplify digital transformation with confidence, speed and agility. For more information, visit IngramMicroCloud.com.

Ingram Micro Inc.
3351 Michelson Dr #100
Irvine, CA 92612

Inquiries
1.800.705.7057
cloud@ingrammicro.com

Customer Support
1.844.256.8346
IMCloudServiceDesk@cloud.im