Dataquest

Your Performance
is our priority

solarwinds msp

EBOOK

GDPR 101

Key Information MSPs Should Know

With the Global Data Protection Regulation (GDPR) set to be implemented in May 2018, IT consultants and managed services providers (MSPs) have been wondering how the new law will affect them. In many cases, the IT press has treated this new regulation with a mixture of panic and consternation. It certainly makes sense—it's a new law that requires organizations to step up on their security measures or face potentially hefty fines.

In this eBook, we'll cover some key aspects of GDPR and how they apply to MSPs. We'll talk about some of the challenges ahead and, hopefully, allay some of the fears you might have about how to approach it in your business.

Key Information about GDPR[1]:

1. Increased Fines
2. Clear, Explicit Consent for Data Usage in Marketing
3. 72-hour Data Breach Notification for Data Controllers
4. Expanded Geographical Coverage
5. Shared Liability
6. Right to Erasure, One of the Enhanced Rights of a Data Subject
7. Streamlined Data Legislation
8. Data Transfer Security
9. GDPR Enforcement
10. Universal Penalties

1. Increased Fines

Although the Fear, Uncertainty, and Doubt (FUD) dial has been set to "maximum power," you can mitigate a lot of issues by taking the law seriously.

In a blog post published on September 15, 2017, Elizabeth Denham, Information Commissioner for the UK office of the Information Commissionaire (ICO) suggests the FUD is "scaremongering." She goes on to say, "The ICO's commitment to guiding, advising, and educating organizations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick[2]."

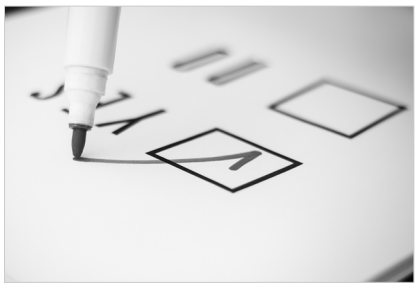
She provides some facts to illustrate this point by writing, "Issuing fines has always been and will continue to be, a last resort. Last year (2016/2017), we concluded 17,300 cases. I can tell you that 16 of them resulted in fines for the organizations concerned. And we have yet to invoke our maximum powers. Predictions of massive fines under the GDPR that simply scale up penalties we've issued under the Data Protection Act are nonsense.[3]" So you may not need to panic, but you absolutely must take the regulations seriously and as best practices suggest, make preparations to follow the guidelines as closely as you can.

2. Clear, Explicit Consent for Data Usage in Marketing

Many MSPs will feel the impact of GDPR in their ability to market their services to new customers. Under GDPR, a company must have a person's consent to send them marketing messages (if the company is not legally able to process the data based upon the legitimate interest legal basis).

Where it gets foggy is when it's a business-to-business communication. GDPR allows businesses to send communications directly to other businesses without the explicit consent of the recipient. This does require some due diligence on the part of the sender to ensure the recipient is "a business." In general, the rules on marketing to companies are not as strict.

For more information on marketing information utilizing the express consent legal basis to process the data, we recommend reading the checklist from the ICO office here: https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf.



Under GDPR, a company must have a person's consent to send them marketing messages.

3. 72-Hour Data Breach Notification for Data Controllers

The 72-hour deadline to report a data breach has added a lot to the FUD around the industry. It's important for data controllers to follow the rule, but there's some nuance to be aware of as well. The difference between a data processor and a data controller is as follows: A controller is the entity that determines the purposes, conditions, and means of the processing of personal data, while the processor is an entity that processes personal data on behalf of the controller[4].

There is a somewhat vague "test" clause in GDPR (GDPR REF) with regards to notification that is more open to interpretation that some people would like. Basically, incidents need to be reported to a Supervisory Authority based on certain risk factors. The office of the ICO suggests:

> *Pan-European guidelines will assist organizations in determining thresholds for reporting, but the best approach will be to start examining the types of incidents your organization faces and develop a sense of what constitutes a serious incident in the context of your data and your own customers*[5].

Given that no specific guidelines have been released, the ICO suggests that organizations consider if the data breach includes the potential of people suffering "significant detrimental effect." This includes, "discrimination, damage to reputation, loss of confidentiality, financial loss, or any other significant economic or social disadvantage[6]."

There is further ambiguity around what must be reported within the 72-hour deadline. According to the GDPR, when the organization doesn't have all the details available on the data breach, they can provide more details after the deadline. As much as the GDPR Supervisory Authority would like to know the potential scope and the cause of the data breach, mitigation actions you plan to take, and how you plan to address the problem, that information may simply not be available. In this case, it appears that you can provide more details outside of the 72-hour window.

It's important for data controllers to follow the rule, but there's some nuance to be aware of...

4. Expanded Geographical Coverage

For MSPs serving companies in the EU/UK from outside the EU/UK (such as the US or Canada), this part of the regulation could cause some concerns.

This is an attempt, not unlike the extension of US Law outside of the jurisdiction of the US, to apply GDPR requirements on any firm that has an EU/UK customer. In theory, it's an excellent idea to extend the rigor and best practices of GDPR compliance to EU/UK citizens' data no matter where it is found. However, it will be interesting to see how and under what circumstances authorities will enforce this part of the law. However, any firm located outside of the EU should take these laws seriously and do what they can to be ready for GDPR.

Any firm located outside the EU should take these laws seriously and do what they can to be ready for GDPR.

5. Shared Liability

Data controller or data processor? Many EU/UK laws tended to place more responsibility on data controllers than they did on data processors, but GDPR has changed this. Both parties now equally share responsibility for protecting Personally Identifiable Information (PII) data.

For the MSP, this is nuanced as it is for most businesses. The reality is that, if responsibility for protection is shared equally between data controller and data processor, spending business cycles determining the roles and responsibilities between an MSP and another party can be wasted. No matter what role your firm plays, it's incumbent upon you to be GDPR ready. So make sure that you work to safeguard all customer information (and employee PII as well).

6. Right to Erasure, One of the Enhanced Rights of a Data Subject

Although there are explicit provisions under GDPR that allow a person to request removal of all their data held by a business—this is known as the "right to be forgotten" or "right to erasure"—this can be challenging for organizations to fulfill. As this right does not apply when personal data is transferred for certain legal bases, the difficulty arises from ascertaining when this right to erasure may apply. Additionally, there are potential technical system limitations to consider.

Many countries require the retention of business records and special categories of personal data. This could cause conflicts where the "right to be forgotten" will conflict with the lawful right to retain or provide access to the records. This conflict often comes into play around healthcare records, legal records, and financial records. For their protection, an MSP should make sure they get a legal opinion regarding governing laws and GDPR compliance prior to permanently deleting business records on behalf of a customer.

7. Streamlined Data Legislation

The overall goal of GDPR was to consolidate the myriad individual EU country data protection laws into a single standard applied across the Union. Although GDPR achieves this to an extent, there are laws that individual countries have passed that could include requirements beyond the scope of GDPR. Germany, for instance, has laws that require that the PII of German citizens remain located in Germany.

The overall goal of GDPR was to consolidate the myriad individual EU country data protection laws into a single standard applied across the Union.

There are other laws in the EU that place geographic restrictions on the storage or transmission of data between countries—often around things like financial and healthcare information. For the MSP providing services to clients in different EU countries, it's important to ensure your backup solution or other tools do not violate geographic location rules.

8. Data Transfer Security

Similar to items 4 and 7, this presents challenges primarily for global companies that transmit vast amounts of EU/UK data in and out of the region. For the MSP, it's important to check that their toolset and third-party suppliers meet the privacy and security expectations set in GDPR.

For the MSP, it's important to check that their toolset and third-party suppliers meet the privacy and security expectations set in GDPR.

An MSP working inside the EU/UK region will need to ensure that the transfer of data is conducted under a data privacy regime, such as the EU/US Privacy Shield or Binding Corporate Rules. Whatever method is selected to execute the data transfer, the privacy of the data transfer should meet GDPR requirements. When the data is "at rest" in a country outside the EU/UK, the rights to privacy should still meet the expectations set out in GDPR. For example, an MSP serving an international law firm may need to implement a specific, secure service to facilitate data to meet the GDPR data protection requirements.

9. GDPR Enforcement

Creating a pan-European data protection regulation like GDPR that requires universal compliance needs an enforcement plan. For the initial phases of GDPR enforcement, this will raise issues as some countries are further ahead in establishing due diligence tests for cybersecurity.

For example, the UK's Cyber Essentials is a government program that prescribes best practices for data protection. Not all EU/UK countries have such a program. Thus, it becomes difficult to enforce a "standard of care" across countries where a "standard of care" has not already been suggested.

UK's Cyber Essentials is a government program that provides practices for data protection. Not all EU/UK countries have such a program.

The MSP looking to implement a baseline for security services and compliance to GDPR should look to an IT security framework for reference. International standards such as ISO 27001 could help demonstrate evidence of "best practice" service delivery. Any evidence that an organization has attempted to implement best practices could possibly help mitigate the severity of assessed fines in the event of a data breach.

10. Universal Penalties

Perhaps the most impactful part of GDPR is its universal attempt to apply "dissuasive" penalties for GDPR violations. As previously mentioned in item 5, the liability for data protection is equally distributed between the data controller and data processor, so it would seem GDPR is designed to aggressively ensure protection of EU/UK data. The law requires that organizations ensure GDPR protection is present, and the PII data is protected and used lawfully and with explicit consent. No matter what type of contract exists between the customer and the business, GDPR remains in force.

For MSPs this has both positive and negative consequences. On the positive side, the MSP and the customer are in the same boat, meaning they must work together to protect the PII data. On the negative side, the MSP must deliver and document in good faith the data protection efforts their services provide. In short, neither the business nor the MSP can contract their way out of avoiding responsibilities under GDPR.

No matter what type of contract exists between the customer and business, GDPR remains in force.

Most MSPs act in good faith and work with their customers. Although GDPR changes some of the approaches MSPs need to take and provides a few challenges for delivering services, MSPs working in the EU/UK will already be accustomed to working with some form of data protection law. GDPR does not need to induce panic—as mentioned earlier, EU authorities have claimed that the.ir intent is still to consider the unique circumstances of organizations. The best advice we can give is to seek regulatory guidance from a legal professional in your country of residence to ensure your services, suppliers, and best practices align with the intent of GDPR to protect EU/UK PII.

1. "Home Page of GDPR." http://www.eugdpr.org/eugdpr.org.html Trunomi, (accessed September, 2017).

2. "GDPR – Sorting Fact from Fiction," Elizabeth Denham. https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ (accessed September, 2017).

3. "GDPR – Sorting Fact from Fiction," Elizabeth Denham. https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ (accessed September, 2017).

4. "Home Page of GDPR." http://www.eugdpr.org/eugdpr.org.html Trunomi, (accessed September, 2017).

5. "GDPR – Sorting Fact from Fiction," Elizabeth Denham. https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ (accessed September, 2017).

6. Breach Notification, Information Commissioner's Office. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/ (accessed September, 2017)