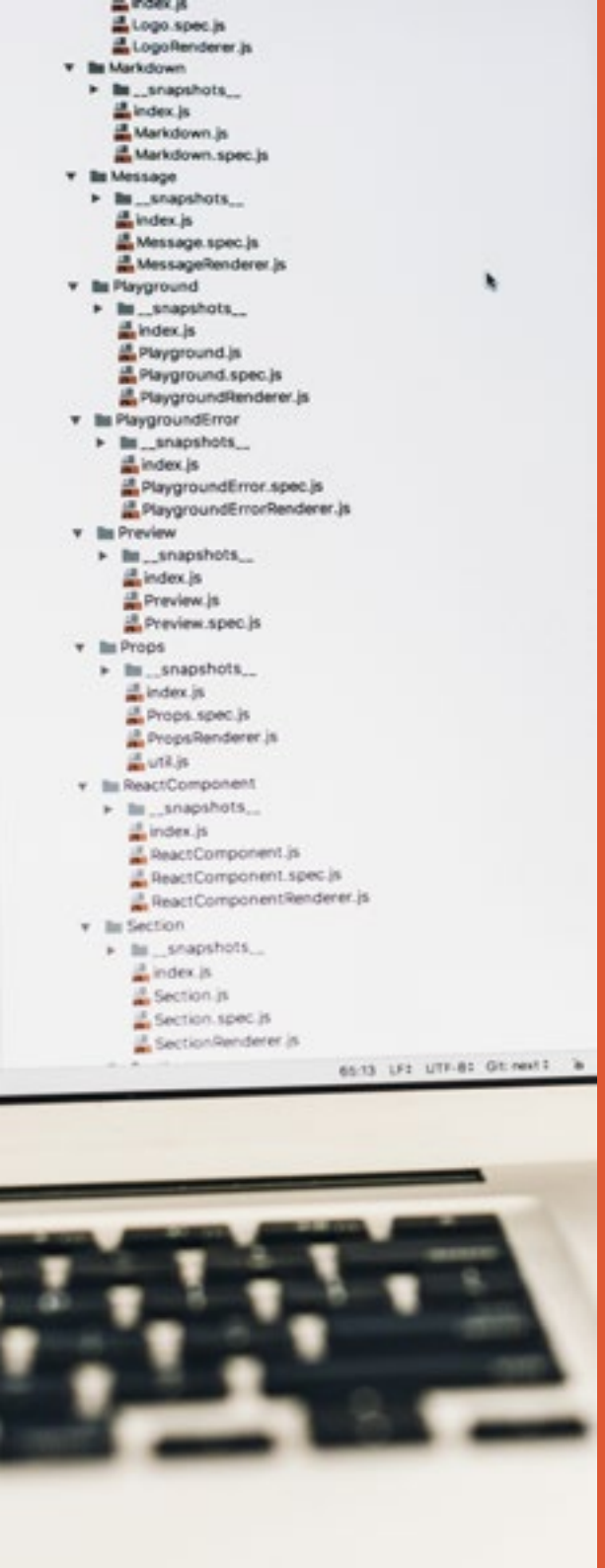


10 Things MSPs Need To Know About The GDPR

RushFiles

Table of content

RushFiles

Introduction

Less than one year ago, the EU Parliament announced the EU General Data Protection Regulation. It quickly became known as the much more idiomatic GDPR. Turns out, however, that actually understanding the regulation is much more tricky.

Almost immediately after the GDPR was announced, rumors and mumbles began to spread like wildfire. The fines are huge. The regulation is far too complicated for small business owners to understand. Companies will have to hire several it specialists and legal experts to reach compliance. And so forth.

This state of, well, mild panic has lasted to this day. And It will most likely increase as we inch closer to the spring of 2018, when the GDPR becomes official law in the EU.

Our goal with this e-book is to help calm the nerves of MSPs all over Europe (and the rest of the world actually - turns out the GDPR is almost indifferent to geographical borders. More on that later!).

Because yes, the fines are huge. Yes, legal matters are complicated and the GDPR is no different. And yes, you might have to spend a couple of hours trying to understand what the heck this thing is all about.

But if you're willing to prepare, the GDPR doesn't have to be that difficult. By reading our e-book you will achieve a basic understanding of what the GDPR is all about and the adjustments you need to make to reach that sweet, sweet state of compliance.

Best wishes,
RushFiles

3 highlights

1 Companies that breach the new EU data protection laws will face severe fines.

2 The GDPR is unbiased. Companies are expected to meet requirements regardless of which sector they belong to.

3 Being a small to midsize business, with little legal expertise, won't get companies off the hook.

RushFiles

Chapter 1:

Why MSPs Need To Know About The GDPR?

MSPs need to pay attention because in this instance the cost of ignorance might be too high to pay. In chapter 9, we will touch on the financial damage that companies might suffer if they fail to comply with the new data regulation. We are not overstating anything by saying that the repercussions would be quite dramatic if any small to midsize company (the standard size for an MSP) were to be confronted with such fines.

The GDPR carries a very big stick, which is one reason to raise your eyebrows. Another one is that the majority of european companies are going to be affected by the new regulations. Most MSPs definitely are. It pretty much comes with the territory when your company is based on a datacenter.

The new EU data law is not sector-specific. Companies from other parts of the world, North America for instance, might be used to privacy laws that relate to just a couple of different industries. That is not the case with the GDPR. It is all-encompassing. And considering the new definition of 'personal data' (we'll get back to his later) and the accompanying 'rights' of all EU citizens (we'll get back to these as well), it is hard to imagine any MSP that won't need to adjust in the near future.

Not only is the GDPR blind to sectors. The data protection laws field the same requirements to small and midsize businesses as to grand multinational companies. Regardless of size, organisational model and staff expertise, companies need to develop procedures for how to comply with the GDPR.

And that, in a nutshell, is what MSPs need to understand about the GDPR: There is really no escaping it.

"The new EU data law is not sector-specific. Companies from other parts of the world, North America for instance, might be used to privacy laws that relate to just a couple of different industries. That is not the case with the GDPR.

Companies need to be able to create an accurate overview of how personal data is processed.

RushFiles

Chapter 2:

The importance of the right software

As the GDPR unfolds in the following chapters, one particular concern might reappear in your thoughts from time to time. Some increasingly frustrated variations of 'We're a fairly small company. We don't have a legal department. We don't even have a legal advisor. How on earth are we supposed to comply with all of this? It's just not doable'.

And hey, these feelings are not completely unwarranted. It took the EU four years of preparation and debate to design this undertaking, no wonder that your palms are getting a little moist. With that said, there are steps that you can take to make the GDPR manageable.

One very important step is to acquire the right software. Now, there is not one single program that we can point to and say 'if you don't purchase this one, you're completely screwed'. Or 'if you buy this one, you are definitely in the clear'. But generally, you need to make a conscious decision about how your company and your employees are going to handle personal data. Part of this process is to find that right piece of software you can trust.

File sharing and file synchronization. Two concepts that unmistakably relate to the GDPR. Your employees are constantly sharing documents and files, working in them simultaneously. Sometimes, these are going to contain personal data. The minute your costumers and their employees store or handle a file or a document that contain personal data, you enter GDPR territory.

Companies need to be able to create an accurate overview of how personal data is processed. An important requirement of the GDPR, one that we are going to return to, is the ability of companies to document their actions. At all times, companies should be able demonstrate how their working methods support the requirements of the GDPR. The best sync and share solutions keep track of who

3 highlights

1 A professional file sync and share-software is an important tool as companies try to comply with the GDPR.

2 Employees need to process and share files within a certain structure for the company to maintain control over personal data.

3 Companies don't want employees to develop their own standards for how to share documents and files.

RushFiles

Chapter 2:

can access files and documents, in what capacity and how each file and document is processed. Absolutely vital stuff to stay in compliance with the GDPR.

It is basically a matter of control. The right piece of software will provide companies with the ability to keep their personal data in check. If a leak were to happen, at the very least companies should be able to identify the breach and correct it. An ability to backtrack is definitely going to make a difference when data protection authorities determine the size of a potential fine.

On the other hand, companies run all kinds of risks if they fail to deploy a professional piece of software. Employees will begin to develop their own systems for how to share and synchronize files, most likely with little regard to data security. Many people work with a gradual transition from work computer to private computer, and if employees don't have a certain structure, including a specific piece of software, to work within, it is impossible to tell where personal data might end up.

The best way to maintain control over personal data is commitment to a professional sync and share-software and make sure that all employees use it diligently.

3 highlights

1 All companies that offer goods and services to individuals in the EU are governed by the GDPR.

2 Companies are grouped in two categories: 'Controllers' and 'Processors'. Processors face the most strict obligations in terms of keeping records of personal data and data processing.

3 'Controllers' must only appoint 'processors' that are able to guarantee lawful processing of personal data.

RushFiles

Chapter 3:

Which Companies Are Affected By The GDPR?

The GDPR is far reaching, in the most literal sense, actually. It doesn't even matter if your company is actually located in the EU. The deciding factor is EU citizens. If your company offers goods or services to individuals in the EU, it is held accountable to the standards of the GDPR. Regardless of whether company headquarters are located inside or outside the borders of the European Union.

So that's that ain't it? Well, if we were to dig a little deeper, we might be able say something slightly more specific about companies and how they are affected by the GDPR.

The most important aspect to understand is that under the GDPR, companies are grouped in two separate categories. 'Controllers' and 'Processors'. Which category your company is located in will determine what it takes to comply. In pedagogical terms, 'controllers' decide how and why personal data is processed. 'Processors', on the other hand, act on the controller's behalf.
Companies that are considered 'processors' do the actual handling of personal data. This is the reason why the GDPR places specific legal obligations on processors. Most notably, 'processing companies' are required to maintain records of personal data and actual processing activities. Additionally, 'processors' face significantly more legal liability if responsible for a breach. These obligations for 'processors' didn't exist under the Data Protection Act from 1998.

Oh yes, life as a 'processor' isn't easy under the GDPR. But it ain't exactly a cakewalk for 'controllers' either. Just because processors are responsible for processing activities, doesn't mean that controllers can hang around. 'Controllers' face an obligation to make sure that their contracts with processors are in full compliance with the GDPR. When controllers appoint service providers to process their data, the service provider must only be appointed if the company is able to guarantee full compliance with the GDPR.

The GDPR imposes strict requirements on data processing agreements between 'controllers' and 'processors'. There has been some speculation these requirements are so comprehensive, that the GDPR will make it difficult for 'controllers' to lawfully appoint 'processors'. As a consequence, an increase in partnerships that are based on complex agreements and outsourcing might take place.

One final aspect to keep in mind: All most each and every company is a 'controller'. At the least in terms of controlling personal data that belongs to their own employees.

3 highlights

1 The GDPR's definition of personal data is slightly different than the definition from the 1998 Data Protection Act.

2 The new definition is more simple and meant to cover a broad range of data types, including 'online identifiers'.

3 The GDPR includes data that is classified as 'sensitive personal data'. The requirements for processing 'sensitive personal data' is stricter than personal data.

RushFiles

Chapter 4:

A New Definition Of Personal Data

In the centre of the GDPR is a new definition of personal data. 'New' because it varies slightly from the definition that was established under the Data Protection Act from 1998. 'In the centre' because it pretty much creates the entire premise for how companies should react to data protection laws.

Considering that 1998 was almost prehistoric compared to today's technological and digital standards, it might surprise you that the definition is relatively unchanged. It is changed, however, with the key difference being that the GDPR uses a definition that is much simpler than its ancestor from 98. Simpler and much more exhaustive in its scope. Anyway, let's try to get up close with the two definitions.

Under the Data Protection Act from 1998 personal data relates to an individual who is identifiable "from those data" or "from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller." Under the Data Protection Act, personal data wasn't just names, personal identification numbers or addresses. Any piece to the puzzle, so to speak, was considered personal.

That principle remains live and well under the GDPR. Here the definition is quite simply that 'any information relating to an identified or identifiable natural person' is personal data. Pretty simple, right? If you have data concerning a person it is a personal data. Very little to get wrong there.

With a simpler definition more data is considered personal. Including a vast range of so called 'online identifiers' that weren't nearly as prominent in 1998. Online identifiers include IP addresses and location data. Types of information that many MSPs have lying around in bundles.

In addition to personal data, the GDPR classifies certain types of information as 'Sensitive Personal Data'. The requirements for processing sensitive personal data is stricter than personal data, a concept that is also derived from the Data Protection Act. But once again the wording is slightly different in the DGPR.

Sensitive personal data is defined as data consisting of - deep breath- racial or ethnic origin, political orientation, religious or philosophical beliefs, trade union membership, biometric data, genetic data, health status and data concerning a person's sex life and sexual orientation. Got all of it?

If you possess any of these data, you should tread it with more sensitivity.

Definition
Under the GDPR, any information that relates to an identified or identifiable natural person is considered personal data.

3 highlights

1 The ‘right to be forgotten’ is also known as ‘the right to erasure’.

2 The ‘right to be forgotten’ is not absolute. But considering the circumstances it won’t be difficult for EU citizens to ask for it.

3 Under the Data Protection Act from 1998, individuals had to scale a much higher threshold to be forgotten than under the GDPR.

RushFiles

Chapter 5:

So, What Is The ‘Right To Be Forgotten’?

One of the staples of the GDPR is the fabled ‘right to be forgotten’. It may sound like a cheesy tagline from the depths of Hollywood, but the right ‘to be forgotten’ is one of the vital aspects of the new EU data protection laws. Companies won’t stand a chance of meeting requirements of the GDPR if they fail to understand what it means to ‘forget’ an EU citizen.

The right to be forgotten is also known as the ‘right to erasure’. The concept of erasure may actually provide a much better visual of what the principle entails. EU citizens have the right to request deletion or removal of their personal data. They don’t have to put forth any particular reasons to substantiate their request. If there is no compelling reason for a company to process personal data, they have to delete it immediately.

Stop for a second and think of the consequences. We have already explained the massive scope of personal data in relation to the GDPR. Pretty much any given piece of data that treats an individual is considered to be personal. Imagine what a laborious task it may be to erase just one person from your files. You can almost hear the sound of data managers heads popping all over the continent.

It may provide some relief that EU citizens aren’t granted absolute ‘right to be forgotten’. But then you consider the circumstances that are required to ask for erasure and suddenly it feels kind of absolute. They are as follows:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

The ‘right to be forgotten’ from the GDPR represents a radical change compared to the Data Protection Act from 1998. Under the DPA, the right to erasure was reserved to instances where the processing of personal data causes substantial damage or distress to the data subject. There is no such threshold in the GDPR.

When an EU citizen asks for erasure, it is almost a given that companies and organisations have to provide it.

3 highlights

1 The ‘right to be forgotten’ is far from the only right of individuals in the GDPR.

2 The new data protection laws include six other rights and different safeguards on top of that.

3 The ‘other rights’ of the GDPR are comparable to the Data Protection Act, but the rights of individuals are strengthened.

RushFiles

Chapter 6:

How About Those Other Rights?

The “right to be forgotten” is far from the only right under the GDPR. The new EU data protection laws feature more than seven rights including the big one we have already discussed. Companies and organisations need to prepare numerous processes in order to comply with all of them. Let’s take a look at those ‘other rights’.

The right to be informed explains how companies and organizations are obligated to provide information of how they process collected data. The individual should be informed through a private notice.

The right of access concerns the ability of individuals to access their personal data and obtain confirmation that their personal data is being processed.

The right to rectification defines that individuals have the right to have their personal data corrected if it’s incomplete or inaccurate.

The right to restrict processing explains that individuals have the right to block processing of personal data, so that companies can only store it.

The right to data portability concerns the right of individuals to obtain and reuse personal data for their own purposes on different services and platforms.

The right to object means that individuals can object to processing in fields such as direct marketing and scientific or historical research. Even processing that is based on the performance of tasks in the public interest can be objected.

And finally, the GDPR includes certain safeguards so that individuals can be protected against potentially damaging decisions that are based on personal data but taken without human intervention. This one is particularly important if your business is based on any kind of automated decision making.

Overall, the ‘other rights’ of the GDPR are fairly comparable to the ones found in the Data Protection Act from 1998. If your processing of personal data was already in line with the Data Protection Act, you should be in pretty good position to comply with the above-mentioned. However, individual rights are generally strengthened compared to the Data Protection Act. It would be wise for any company to assume that their current processing of personal data will need some adjusting.

Chapter 7:

Does Geography Matter?

3 highlights

1 Despite the GDPR's intention to harmonise data protection law all over the EU, national law still does matter.

2 Companies that work in several member states need to familiarize with national law - mostly for precautionary reasons.

3 The GDPR is going to be the dominating data protection law across the Union.

Yes, we have already explained that the GDPR covers all companies that offer goods or services to individuals in the EU. So obviously geography doesn't matter, right? Well, actually, it's not that simple.

The GDPR aims to harmonise data protection law across the European Union. However, there are still areas in which Member States can apply their own national rules. These areas may fall outside the union's legislative competence or some Member States have constitutional rules that apply. What it does mean is that data protection law across the EU isn't quite as consistent as the GDPR may have aimed for. Companies that work in several Member States (many MSPs do) will experience different data protection laws from one Member State to the next. So despite efforts to eliminate such headaches, companies still need to concern themselves with the GDPR and national laws alike.

In that regard, it might be a redeeming feature that most legislation across the EU will be subject to the GDPR. For precautionary reasons, companies need to familiarize with relevant national laws wherever they do business. In most cases, however, they will find themselves navigating GDPR territory.

For instance, Member States remain in charge of determining limits of free expression. In some Member States personal data can be processed for reasons that relate to free expression, in other one's it can't. Issues in which national law trumps the GDPR include national security, defence, the investigation of criminal offences and other important public interests. Not to say that the standard MSP doesn't process personal data that relate to important national affairs, but, well, in most cases it probably doesn't. At least not on a daily or weekly (or monthly) basis. And probably almost never in situations, where the company won't naturally cooperate with authorities during serious national crisis.
Not all exemptions from the GDPR stem from national security and similarly heavy stuff, however. For an example, members states are free to determine their own law regarding the processing of national ID numbers. Employment laws are almost exclusively outside the legislative reach of the EU including the relevant personal data. And in some Member States, certain sectors (such as law firms and banks) are subject to specific obligations in terms of professional secrecy. And this is just a fragment of national law that is going to be around despite the GDPR.

In other words, MSPs, you have no choice but to pay attention to national law in all the countries you roam. Despite the fact that having a thorough understanding of the GDPR will most often have you covered.

Chapter 8:

What Does Compliance With The GDPR Even Mean?

MSPs who dream of a quick fix or one-time solution are going to be sorely disappointed. The ability to comply with the GDPR is going to require a continuous effort. The reason is perhaps the most significant addition to the GDPR compared to previous data protection legislation. Including the Data Protection Act from 1998.

That addition is the new 'accountability requirement'. The important thing to understand is that companies are required to demonstrate how they comply with the key principles of the GDPR. Companies will need to update how they approach and process personal data on a constant basis. Each time working methods are changed, new types of customers are brought along or personal data registered in a new way, companies need to keep the protection of personal data up-to-date. Otherwise, they won't be able to demonstrate to relevant authorities how their working methods are in compliance with the GDPR.

To comply is to document that you respect the data protection principles of the GDPR. Those principles include that personal data is processed 'lawfully, fairly and in a transparent manner in relation to individuals'. They also dictate that personal data 'should be collected for specified, explicit and legitimate purposes'. And personal data should never be 'further processed in a manner that is incompatible with those purposes'.

MSPs will need to start preparing right now if they want to comply by the spring of 2018. Perhaps the most effective approach is to break the concept of compliance into small pieces. We suggest the following route:

The important thing to understand is that companies are required to demonstrate how they comply with the key principles of the GDPR. Companies will need to update how they approach and process personal data on a constant basis.

3 highlights

1 The ‘accountability requirement’ asks that companies are always able document how they comply with the data protection principles of the GDPR.

2 Because of the ‘accountability requirement’ compliance is going to be an ongoing process for companies.

3 MSPs will need to break compliance into small pieces. The first step is identification.

RushFiles

Chapter 8:

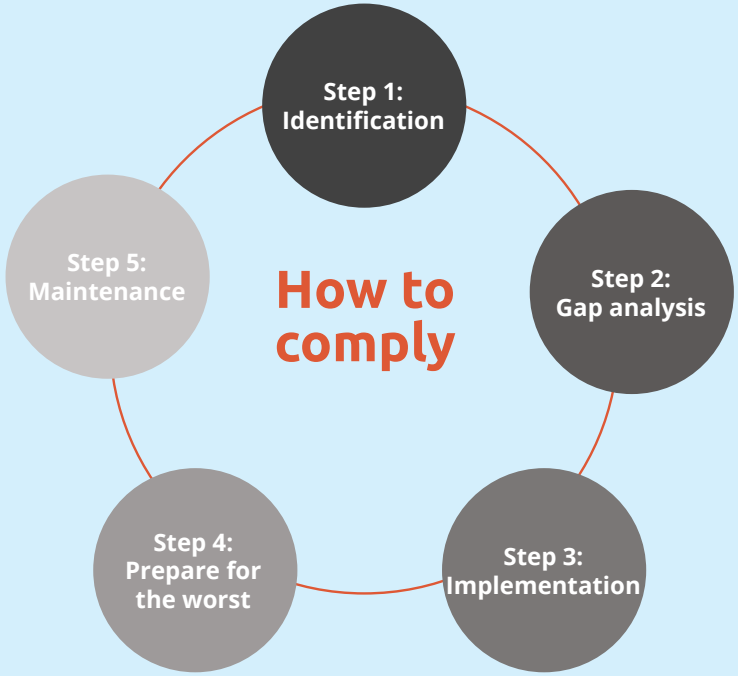
1. Step: Identification
In the opening phase, companies need to create an overview. All of the company’s data should be mapped. Where is data located, who can access data and what purpose does it serve to the company?

2. Step: Gap analysis
Quite simple but also quite extensive. In the second phase, companies compare their findings from the identification phase with the actual requirements from the GDPR. This process will make clear which steps are needed to comply.

3. Step: Implementation
Another big one. Companies now have a thorough understanding of their personal data and the gap between current procedures and those needed to comply with the GDPR. Organisations that didn’t pay much attention to the DPA will have a huge task right here, but the job is to implement the principles of the GDPR in working procedures.

4. Step: Prepare for the worst
In case of a breach or leak, how is the company going to respond? Procedures should be in place to identify what types of data were leaked, which parties leak involves, what are the consequences and how can we make sure that it doesn’t happen again?

5. Step: Maintenance
We’re back at the ‘accountability requirement’. Companies need to make sure that safety procedures are coordinated with business activities. A constant effort.



The GDPR clarifies that in cases of a minor infringement, a reprimand could be issued rather than a fine.

RushFiles

Chapter 9:

What Punishment - And How Hard Will It Be?

When the GDPR was disclosed in early 2016, one aspect caught the attention of companies and organisations like none other: The sheer volume of the fines that 'controllers' and 'processors' could face if unable to comply with the GDPR. And it is true, actually. Fines have increased drastically compared to the Data Protection Act from 1998.

The GDPR sets out a maximum fine of 20 million euros or four percent of the company's worldwide turnover. According to legal experts, the increase could be the biggest game changer compared to the Data Protection Act. The theory is that companies and international coperations will be forced to pay attention.

Still, there is an element of consideration in how the fines are meted out. The standard MSP would have to screw up quite royally to trigger fines worth seven to eight figures. Under the GDPR, administrative fines are 'discretionary rather than mandatory'. It means that they are imposed on a case by case basis and according to the GDPR's own phrasing administrative fines must be 'proportionate'. Companies are expected to establish comprehensive, but proportionate governance measures.

If you're careful and committed to comply, you're probably not going to face a really heavy fine even if a breach or leak were to happen. In fact, the GDPR clarifies that in cases of a minor infringement, a reprimand could be issued rather than a fine.

Factors that will be taken into account when determining if a fine will be disposed (and the amount of that fine) include the nature and gravity the infringement, whether the infringement is intentional or negligent and actions taken to reduce the damage suffered by individuals. The willingness to cooperate with supervision authorities will also be taken into account.

Enforcers
National Data Protection Authorities (DPAs) are in charge of implementing and enforcing the GDPR.

DPAs have the authority to regulate all kinds of organisations and all types of business activity as long as personal data is involved.

3 highlights

1 The risk of eight figure fines has stolen much attention in regards to the GDPR. However, fines in the range of millions of euros will require very serious violations of the GDPR.

2 Fines are proportionate and given on a case by case basis. Some infringements will result in a reprimand, not a fine.

3 The right of individuals to ask for a remedy could challenge companies.

RushFiles

Chapter 9:

This is not to say that 'controllers' and 'processors' won't face any punishment as long as they're not huge international conglomerates and keep a positive spirit about the GDPR. But the idea of Data Protection Agencies handing out fines worth millions of euros left and right is not overly realistic. At least not as long as companies make a serious commitment to compliance, and make sure not to sweep breaches or leaks under the rug. Explicit damage control is another way to lessen fines.

An interesting aspect of the GDPR is that individuals, who believe that their rights have been infringed, can ask the 'controller' to remedy the situation. If the individual does not receive a sufficient answer from the 'controller', he or she can decide to file a complaint to the national Data Protection Agency. The Data Protection Agency is required to keep the individual informed on the outcome of the complaint.

Now, regardless of the specific outcome, just the right of individuals to make such requests is going to put a strain on companies. And if they fail to provide sufficient answers, Data Protection Agencies will notice. Therein lies one of the more unpredictable elements of the GDPR, and perhaps the greatest risk of committing a violation for most MSPs.

An interesting aspect of the GDPR is that individuals, who believe that their rights have been infringed, can ask the 'controller' to remedy the situation.

Chapter 10:

What Will Happen On May 25, 2018?

3 highlights

1 The GDPR was published by the EU Parliament on 4 May, 2016. After a two-year grace period, it will be enforced on May 25, 2018.

2 Companies are expected to be in compliance by the end of May next year.

3 Privacy Impact Assessments and harmonised breach notification laws are two key issues that companies should be ready for come May 25.

It has been described as D-Day for data protection law in Europe.

On May 25, 2018 the GDPR will apply in all Member States and globally to all companies and organisations that offer goods and services to individuals in the EU. And this time there is no fooling around.

The GDPR was published by the European Parliament on 4 May, 2016. Unbeknownst to most people it came into force just twenty days later but the introduction was followed by a so called two-year grace period. Effectively, companies were given an opportunity to prepare for the GDPR. However, one has to wonder if some decided to push the objective of compliance as far into the future as possible. One year's time has passed and many companies may start to feel like that D-Day is moving closer and at a rapid pace.

When owners and employees working at MSPs wake up on a that fateful spring morning, it might be wise to keep in mind a list of initiatives that should be started up immediately to comply with the GDPR. For instance:

New rules for consent

MSPs that use consent as their primary legal basis for processing personal data, should be aware that the standards for consent have been considerably heightened under the GDPR compared to the Data Protection Act. Companies need to review their consent mechanisms to make sure that they meet the requirements of the GDPR.

Privacy Impact Assessments

Shortened PIAs are a concept that companies might as well familiarize themselves with. Under the GDPR, companies are required to conduct privacy impact assessments any time they launch a project that implies an increased risk of personal data breaches or leaks. As projects progress, companies need to stay in compliance with the DGPR.

Contact within 72 hours

EU Member States have represented a variety of different data breach notification laws, but that is about to change under the GDPR. The GDPR wants to harmonise data breach notification laws by requiring that companies and organisations notify their national data protection authorities within 72 hours of discovering a data breach. Companies need to ensure that they have the necessary technology and working methods to identify breaches and notify the relevant authorities.

Companies that are yet to begin their preparation for the GDPR, will have plenty of work on their hands in the upcoming 12 months.

From May 25, 2018 the GDPR is reality all over the EU.

RushFiles

RushFiles