BELGIUM CHAPTER
20 Years 1998-2018

What a PM should know about GDPR

Interview with Kris Troukens
Interview by Frank Turley
Date: March 2018

I: Hi Kris, thanks for making the time to discuss: What a PM should know about GDPR. My first question is where did GDPR come from and when will it go live?

R: GDPR is the new privacy law which will come into force on 25/05/2018. It will replace previous existing privacy laws which dated back to '95. In 1995, we did not have Google, Facebook, smartphones, RFID's, etc., all of which collect lots of data from their customers. The European Union wants to enforce this new law, which was approved on 25/05/16. We are currently in the preparation period, so companies should have started thinking and working on this two years ago. Today we are in the grace period.

I: How many companies have actually done something about this, do you think?

R: Well, I see that there's a lot of things happening. First the big players, Google, Facebook and Cloud providers (SAP, Oracle, etc.) are really busy completing their preparation. If you do a google search for "Amazon GDPR", you will find details about their conformity program. So the big players seem to be taking action.

Then you have the next set of companies, which I would call larger companies. For example, in Belgium, you have the larger banks, insurance companies, etc. They are well advanced on their compliance program, but then there's a whole lot of small and medium-type businesses and they're only just waking up and I speak from experience. I'm helping companies get compliant and my phone hasn't stop ringing since New Year.

It is important to note that the privacy commission is likely to be concentrating on larger corporations first to see if they're following the GDPR rules.

I: What's an easy way to check if a company is obeying the latest laws?

R: Have a look at their privacy policy on the website and if you can see that, the new requirements as dictated by the GDPR are already translated in some statements in that privacy policy. If that is the case then you can be pretty sure that they're well advanced with their preparation.

On the other hand, what I see frequently with customers who are contacting me is I go to their website and have a look and either there is no privacy statement - big trouble - or they have a completely outdated privacy statement and then obviously there's still a bit of work to be done.

I: What do companies have to do to support their privacy policy?

R: Well, the privacy policy only shows one side of the story. The true story is behind the scenes. Are they really doing the stuff, putting the procedures in place, etc., etc.

I: How is the government going to work? Are they going to hire a lot more people?

R: Well, it is the duty and the task of the Privacy Commission in Belgium to check if everything is running smoothly. They advise customers who are having difficulties or have questions. They also advise customers who want to file a complaint and offer assistance. , However, a couple of months ago, they were clearly under-staffed with all their own preparation work.

I: Can you explain the 'right to be forgotten' in this privacy policy?

R: In the privacy policy, any customer or client has some new rights and one of them is "the right to be forgotten". So you can contact any company that you think is keeping personal data relating to you and ask them for a copy. Or you can check what data they have on file. And you have indeed the right to be forgotten, i.e. to be erased from their system. So that initially raises an interesting question. In what system does that data reside and are those systems and software ready to erase one record on demand of a customer? Another interesting question is "can you just erase that data", because there may be legal reasons why you need to hang on to that data for X number of years, for example if you need to re-print past invoices, … It raises a lot of questions and a lot of concerns.

I: So if you have a website, a client can ask, "What information do you have on me?"

R: If it's a simple request for information or request for a copy of all the data you are keeping on them, you have 1 month to reply. However, there's another important deadline. If you have any kind of data breach, especially with your HR data which is stolen on the subway for example, then you have to inform the Privacy Commission and any potential customer that may be impacted by that theft and you have to do that within 72 hours, which is a very short time to do so. So you should already be thinking about procedures on how to do this , which person to call, which website you should be filing your stuff in, etc., etc., and so you should be ready before you start to receive requests

I: My next question was going to be what should every Project Manager know?

R: A couple of things on the Project Manager side. Some companies are saying to me: "We are certainly not concerned as we don't have all that much personal data." I then ask:

- "Do you have employees?"
- "Do you have staff on your payroll?"

I then remind them that GDPR applies to you because you are also collecting personal data from your staff and even more so, you're collecting sensitive personal data. Just think about the medical checks, family information, bank details, yearly reviews, payroll data for each employee. This is very sensitive personal data and you need to look after it.

As a Project Manager, you should at all times be thinking about privacy when you're designing new systems, new databases, new platforms, etc. You should keep personal data in mind. You should only capture it for one particular reason, which is the fulfillment of the contract that you have. For example, in a hotel, I sell a room, you pay for the room. That's the contract. So in order to sell that room, you need the name and the birth date and a couple of other details from your guest, so that's covered under the contract. After the person leaves the hotel (contract is fulfilled), you no longer have legal obligations to keep that data, so the software should remove the data it no longer needs.

Many companies think they can use all this data for electronic newsletters, which is not correct. That was not the purpose for which you have collected that data. That customer came to you for another reason and they were never signed up for a newsletter.

I: What about cloud services where the servers are located outside Europe?

R: Data as long as it resides within the European Union is fine. There are a couple of other safe harbor countries where you can store your data such as the USA. There is an official list of all these countries, but if you are going outside one of those countries, then you should seek legal advice as you will need it.

I: What about the cloud services offered by Microsoft and Amazon hosting?

R: It is always best to check the latest statements because these statements are regularly changing as we are approaching the 25th of May, but for sure the big players, Amazon, Google, Microsoft, they have been setting up large data centers within the European Union zone just for this very same reason. I am a customer of an online platform, which is called Zoho. A year ago, when you signed up for Zoho, you were transferred to the States. Today you log in to zoho.eu. So that clearly shows that all those big players are hosting data now within the European Union because they have to. They just have to.

I: Can you name some safe harbor countries?

R: I have the list here in front of me actually. Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the United States. So those that I mentioned are okay because there are proper agreements in place between the European Union and these countries. If you have data hosted elsewhere, then it's going to be tricky and I advise you strongly to seek professional assistance.

I: What kind of fines are going to be in the pipeline for this if …?

R: Fines can be up to 20 million Euros or 4% of the annual global turnover. So if you have a company which has a small turnover, under 20 million, then they could be fined up to 20 million if they breach a number of the rules. However, the Privacy Commission will start with warnings and you will be asked to show that you have done your homework in preparing correctly with your GDPR compliance program. If you are a worldwide company like Facebook, then 4% of your world turnover can be a few billion euro.

I: Thank you, Kris. How can people contact you if they have more questions on GDPR?

R: I have a website and a couple of interesting GDPR checklists and articles that you can consult and download as well, and that website is **www.qhotelservices.com**.