

# The GDPR, our journey from risk to opportunity.

And suddenly... everyone is a Privacy specialist. IT Consultants, Law Firms, Risk Management Consultants, free-lance Data Protection Officers, ... But how does a company really organize itself for this upcoming new Privacy Law? Is there truly a quick fix?

In a series of questions to Jan Moers, privacy specialist within Nestlé Legal, Benelux, he looks back on our own journey and shares with you our experience. We hope you recognize some of your own stories and lessons learned while reading this.

## KS: JAN, HOW DID THIS ALL START?

JM: Let's go back to March 2015. On the horizon the GDPR was showing up. At that point in time, privacy legislation was not really top-of-mind for most people. Not even within the Legal Community. Of course, privacy counsels existed. But you'd find them more often in banks and telecom companies. Personally, I had no solid background on Privacy whatsoever. I had been working first as a lawyer in a law firm, a legal counsel in a bank and as a spokesperson for a consumer organization.

Rather naively, I took on board the challenge to prepare our company for this upcoming legislation. Luckily, I had a visionary manager who understood that we'd better prepare ourselves in time. Our first plan? Do a mapping exercise, identify the gaps and mitigate. Simple, isn't it?

Very soon I noticed that this could not be a one-man's job. The amount of data, the complexity of the processes and most importantly the multidisciplinary character of the issue would require some kind of superman to achieve compliance solely.

## KS: SO, WHAT DID YOU DO?

JM: Therefore, we needed to reach out to other stakeholders. Comes in, my partner in crime for the next few years, our IS/IT guy. I remember those first meetings vividly. How do you put a legal & IT guy in one room with the objective to create an

alliance on an issue that has both legal as well as IT aspects in it? IT and Legal sometimes seem to live on different planets. In my case personality also played a role. How do you forge a solid partnership between a 30 year old rascal and a 60 year old rebel?

I was lucky. At first, our IS/IT guy, Ben, was a little bit hesitant when I said that we needed to sit together. What the h\*ll did Legal had to do with all of this? I think he was as wary as I was. But very quickly, a common understanding started to develop. We still spoke different languages of course, but we started to share the same objective and it wasn't compliance on privacy legislation that was our main driver.

## KS: IF COMPLIANCE WASN'T YOUR DRIVER, WHAT WAS?

JM: As I was taking on board the mapping exercise, I noticed something very odd. I grew an interest in the possibilities of using personal data. After all, in order to protect data, you first need to have data. It should not be that only the Google's, Amazon's and Facebooks of this world explore the enormous potential of personal data. Ben, working on IS/IT projects, knew and understood this long before me. He understood the power of data and was more than keen on working to exploit this in a positive way for our company.

We started to reflect on how the new legislation would impact our ability to USE personal data. As we were now meeting very regularly, we thought it would be good to give our newly born alliance a name. After all, every child needs a name. And so, the 'Digital Core' Team was created. At first we wanted no structural set-up. Who needs another formal vehicle, right? However, right after several weeks of seeing each other at least once a week, we understood that in order to be taken seriously and maximize our impact we needed to formalize our meetings and have them weekly. We never stopped since.

## KS: SO LEGAL AND IT PLAYED THE STARRING ROLES?

JM: These first meetings were still very unstructured. At the same time we did some ad hoc work. Working together on a cloud supplier, dealing with personal data for example. But we always came back to the same conclusion. What's the point

of this, other than using personal data to its full potential? Of course, taking on board the appropriate amount of respect for the individuals behind the data. After all, we didn't want to create the next Big Brother.

And so our attention turned towards another stakeholder. Enters Marketing & Communication. Somehow we succeeded in explaining to them the importance of compliance related to this topic. Finally, we had found our partner inside the business to set this thing on the right track. Our Digital Core Team grew with one, so three people met on a weekly basis discussing ad hoc topics, but also started to think on how we could align on long term projects.

And yet. It was not enough. Something was missing. How do we spread the message throughout the whole company? How do we create enough body and importance to this 'Digital Core Team' in order to be able to advise, steer and even block business when necessary?

It became clear we needed external advice in order to set up a strategy and governance. We started to brief our local management committees and tried to make clear that resources should be made available to ensure this. Things got serious. We had to talk about money...





### **KS: HOW DID YOU CONVINCING THE MANAGEMENT COMMITTEES, WHICH WAS PROBABLY NOT AN EASY TASK?**

JM: We understood that asking for resources would mean that we had to bring a compelling story. Only focusing on the compliance aspect of this, would bring us only so far. We needed to convince them of the fact that investing in a strategy on personal data and building a governance structure is essential for business success. The GDPR, with its principles on purpose limitation (only use personal data for the purpose you defined) and accountability (demonstrate you are organized) now forced us to maintain a coherent and effective approach.

This huge risk, which was - and still is - a future risk, presented us an enormous opportunity at the same time: all Nestlé businesses using personal data to its full potential, and trying to become the most trusted FMCG company. This was the message we got across, in two countries.

After a few months a formal decision was made to send out a briefing to outside consultancy firms.

### **KS: I ASSUME THERE WERE QUITE SOME ADVISORY FIRMS THAT WANTED TO STEP IN?**

JM: At the time, a lot of consultancy firms were still focused heavily on the security aspect of Data Protection. Although this is of course important, it was not what we were looking for. We wanted to find a company that believed in the commercial value and power of data and would use this as a starting point to ultimately achieve compliance. Not the other way around.

After we found our partner it took us almost a year before the job could start. The complexity of rolling this out at the same time in both countries and the financial impact which became tangible were causing this. In hindsight, this delay was a gift. With every month passing by, our internal organic organization became more and more effective and mature. By the time, the consultancy firm visited our premises for the first time, we had a very good idea of what we wanted and what we didn't need.

This doesn't mean that such an exercise goes smoothly. It took two internal project managers and the consultancy firm two months to go from a lot of interviews and workshops to deliver a personal data strategy and a personal data governance. In that order. Then we had to align this with the decisions and structures that were being set up from a Nestlé Group perspective.

We now had formalized a strategy enabling us to strike the balance between using and protecting personal data. Within that strategy, governance is a key point. This governance system is one where the multidisciplinary team (the previous digital core team) transformed in the Personal Data Core Team. It has the duty to advise and the power to block when it deems it necessary. Marketing is leading the show. In addition, there is a network of SPOC's throughout the different divisions of the company, called Personal Data Ambassadors, which acts as a Personal Data Community.

### **KS: WITH A PERSONAL DATA STRATEGY AND GOVERNANCE ON THE TABLE, THE CORE TEAM COULD HAVE SOME REST?**

JM: No, not at all. During all this time, we did not sit still. Project plans were drafted, data registers were build, suppliers were assessed and the weekly meetings with all stakeholders went on. We had different speeds at different moments as priorities shifted and people changed, but we never lost track of what was needed.

We kept on, driven by our purpose to ensure that business would be able to USE personal data within a secure and legal framework.

We are now March 2018. Three exciting years seem to have passed by in a hurry. In a few months, the GDPR will go into effect. Business as usual. But I am in no way worried. It's so satisfying to see how all of our preparation now is leading to tangible results. Our Personal Data Ambassadors are becoming personal data enthusiasts with the appropriate respect for the person whose data we process.

After three years, it can finally truly begin...

### **KS: THIS IS A VERY INTERESTING, WARM AND 'HUMAN' STORY OF OUR PERSONAL DATA JOURNEY, JAN. CAN YOU SHORTLY SUMMARIZE THE LESSONS LEARNED?**

1. Invest in your relationships with others  
As with most things in life, Privacy compliance is something you achieve as a team. It is important to invest in this team. To get to know your key partners. You will be spending a lot of time with them.
2. Take your time  
It is very difficult to get everything right the first time. In fact, we needed the blocks on the road to accomplish the journey together. Don't get too easily disappointed if it doesn't go fast enough. Especially if you have to bring people up to speed, slow is usually the most durable way to go.
3. Focus on the opportunity, not the risk  
Most people are not getting satisfaction for being compliant as such. It's your job to make them see the opportunities of a situation. First think about possibilities and set boundaries after. Don't start with 'you can't', but with 'what if we...'
4. Beware of the GDPR / Privacy specialist  
In my humble opinion, the only GDPR specialist I would trust is the one who is not selling me answers. As we speak the GDPR is not even into effect. A lot of uncertainties are still to be clarified. Take this time to get organized and get help with that. You can only take one step at a time in an important process as this.