Novartis Privacy Head (EU): 'We Need to Manage the Grey Zones in the GDPR'

The IAPP Europe Data Protection Congress is taking place on 18-21 November in Brussels and as its media partner the European Data Protection Law Review (EDPL) is featuring interviews with selected speakers of the event. In the following conversation **Alexandre Entraygues**, **Novartis Privacy Head (EU)**, shares what are some of the challenges and lessons learned from the perspective of a privacy professional working in the pharma sector. EDPL's executive editor, Nelly Stratieva, conducts the interview.

NS: Alexandre, you're in charge of privacy matters for the European market for Novartis, one of the largest pharmaceutical companies in the world. What privacy and data protection challenges will be keeping you busy in the near future?

AE: As a matter of fact, the amount of work has never ceased growing since I joined the privacy function at Novartis. It can be attributed to external factors like GDPR or new local requirements, but also to internal factors like the increasing importance of data and digital at Novartis or the increasing maturity of business stakeholders in privacy-related matters. It can be therefore reasonably predicted that I will remain busy and even busier than ever in the near future, just like other privacy professionals at Novartis.

Now, if I have to name the highest privacy challenges which are coming to me, I would pick up three. First, as any other company operating in Europe, Novartis has to find its way to manage the grey zones in the GDPR, where the text is silent or unclear, and where the existing guidance is insufficient. Because this grey colour is not only a bunch of small drops on some tiny details but actually covers such critical topics as defining the privacy roles as controller, processor, or joint controller when sponsoring clinical trials, when launching patient support programs, or when conducting market research. Interestingly, there used to be a detailed opinion issued by the Working Party 29 in 2010 but it turns out that this opinion is not in the list of those which were formally endorsed by the European Data Protection Board so far.

The second challenge which will keep me busy in the near future is defining the conditions for making use of existing data in order to upgrade or enable therapies which will improve and extend people's lives. Such use may include developing or applying machine-learning algorithms - which already pose new and unique legal and ethical questions - and does require standards for assessing compatibility of different purposes.

Finally, my team and myself will always be busy in partnering with other functions within the organization to help them becoming more mature in data privacy, understand the risks they are facing in their daily management of data, and help them put in place targeted and efficient controls to manage these risks.

NS: At the 2019 IAPP Europe Data Protection Congress you'll be speaking about clinical trials as a story of trial and error. Could you share an example or a best practice from your own experience at Novartis?

AE: Being a privacy professional these days is, by definition, a learning experience. Privacy is a field which has been under (re-)construction for the last five years, and a lot of the long-lasting assumptions had to be revisited. So, to pursue the analogy with clinical trials, I could provide a lot of examples where an approach was taken, tested and then amended or reconsidered in order to bring improvement or fine tune the initial options.

When I think about the relationship to the other functions within my company and how we are making sure that all projects coming in are being assessed from a privacy perspective, this is probably a good example. We started with a traditional approach, developing awareness of operational teams through communications and trainings, expecting them to populate our privacy management platforms so that we are able to make proper inventories and assessments. But then we realised that this was not enough. That we needed to be more proactive ourselves, initiate conversations with the business from a different angle, and look deeply at their daily processing activities, habits and procedures, how they were collecting data, storing data, securing it, sharing with third parties and how they were reacting when their databases were breached. Accordingly, we decided to implement an approach which was no longer based on projects, but based on functions and teams. The idea was to reach out to these different functions like Finance, Legal, HR, etc, take time with them, and join our efforts to highlight their key privacy risks, document their procedures and controls, and potentially agree on certain new controls which needed to be put in place. This is one example.

Another example that comes to mind when thinking about a process which was developed and improved over time is the mapping of data flows in the context of clinical trials. I joined Novartis three years ago as Head Data Privacy for France. As many of us know, the French regulator, CNIL, anticipated on the GDPR requirements as early as 2016 when they issued a revised version of their framework for clinical trials, the so-called méthodologies de référence (MR). These MR were introducing a set of new requirements including that the sponsors map the data flows involved in their clinical trials. In order to meet this requirement, we first had to put a lot of efforts in developing a local template and then in educating teams in charge of data management so they understand the need and they are able to populate the fields. It goes without saying that the process required a lot of back and forth and to be improved in order to fit the different scenarios. At a certain point, when the process was finally adopted, we decided to extend it to other European countries so that it eventually becomes a GDPR standard.

NS: Healthcare is a sector that deals with sensitive data and at the same time develops life-saving innovative products, often employing cutting-edge tech that might have major impact on privacy. How do you balance these different societal interests in your job? How do you make sure we reap the benefits of innovation without sacrificing privacy? Or is it an illusion to think we can have both?

AE: I don't think that it is an illusion. We can have the full potential of innovation and, at the same time, ensure a responsible use of data.

I believe that one key condition for enabling this virtuous combination to happen is that privacy professionals like myself look at the cutting-edge projects at the very early stages of their development (privacy by design) and then make the effort to be innovative also in protecting privacy. In practice, it means that we apply the utmost curiosity, asking as many questions as necessary so that we fully understand the business needs. After this first stage, it is our time to be innovative in order to match these business needs, and this often requires questioning the status quo. A good example of that approach would be the legal basis to process sensitive or non-sensitive data. For ages, consent was considered as the golden standard for privacy, and you could not review a single break-through technology project without being asked how we would collect data subjects' consents to make that project possible. We, at Novartis, worked hard to establish processes and develop arguments so that consent would no longer be the ABC of privacy in our company. Of course, this required demonstrating the value of alternative grounds, including the legitimate business interest we may have in processing certain types of data. And it was hard to explain how legitimate business interest could actually, in certain cases, be more protective for the individuals, because it implies a thorough analysis documenting how we balance the business goals of the company with the interests or fundamental rights and freedoms of the data subjects; in the end, it implies making sure that the technology takes into account the interests of the data subjects at stake and is accompanied with the right protective measures. And the same goes with scientific research as a legal basis to process health data, which requires putting in place specific safeguards like pseudonymisation or contractual obligations, which will enhance the privacy of the patients. Conversely, when you look at consent as a legal basis, you realise that it often provides the illusion of self-determination and protection, while the individual may actually not always read the information provided, may not always understand this information, and may not be in a position to refuse anyway.

These considerations are probably among those which led Brad Smith, the President of Microsoft, to acknowledge that we are living the 'third wave' in Privacy: the first wave was 'notice and consent', the second wave was 'access and control', and the third wave which is now showing up will need to include new laws and regulations, as well industry driven standards.

None of these waves, of course, involves sacrificing privacy for the benefit of innovation, or the other way round. If it happens that we cannot have both, then we need to consider anonymisation and see how we can operate in that context.