GDR NEWS

Maja Smoltczyk: The exit interview

Bethan John 27 October 2021

Berlin privacy chief Maja Smoltczyk has become a key player in the European data protection landscape. Shortly before her retirement, she told GDR about the GDPR's successes and failings, how her office reached Germany's first multimillion-euro fine, and its ongoing audit of the aftermath of Schrems II.

First published on the *Global Data Review* website, October 2021

The last five years have been a time of upheaval for data protection in the EU and beyond. What are the most significant lessons to be drawn from your time as commissioner?

The GDPR has undoubtedly ushered in a new era for data protection in Europe. It has created new challenges for data controllers in business and government, as well as for supervisory authorities. It has also fundamentally raised public awareness of the protection of personal data. I have noticed this time and again – in the steep increase in complaints, the many media enquiries and my discussions with controllers in the state of Berlin.

With this in mind, my authority has especially strengthened its cooperation with European supervisory authorities, comprehensively modernised its work processes and carried out various large-scale audits.

Meanwhile, the time since the outbreak of the coronavirus pandemic has shown me the extensive backlog we continue to have in the implementation of fundamental data protection requirements. And this is true in all areas of society - starting with the health sector, continuing with schools and ending with the workplace. In the meantime, important steps have been taken and gratifying successes have been achieved, but there is still an enormous need for action for all stakeholders.

What do you think are the main successes and failings of the first few years of the GDPR?

The first major success of the General Data Protection Regulation was achieved even before it came into force: data protection was suddenly on everyone's lips. Many companies that had previously given little to no thought to data protection compliance began to review their processing procedures and adapt them to the GDPR. This was certainly due in no small part to the new levels of fines.

Citizens have also become more aware of their data protection rights. This was certainly also due to events before the GDPR entered into force, such as the Snowden revelations. Nevertheless, the GDPR has

First published on the *Global Data Review* website, October 2021

significantly strengthened the transparency rights of citizens. In the meantime, many people are not only more aware of their rights. They also know how to enforce them (possibly with the help of data protection supervisory authorities). Incidentally, this is another success of the GDPR: supervisory authorities have finally been given the tools to effectively prevent and punish data protection violations and thus really help citizens.

But the success also has its downsides. As a result of the aforementioned upgrading of the topic, supervisory authorities have also received many more submissions than before. At my authority, for example, the daily submissions and complaints almost quadrupled after the GDPR took effect. At the same time … especially in the technical areas, it is difficult to obtain qualified personnel, as we are competing with financially strong companies (which we are, after all, supposed to control) for the best minds.

To what extent is the GDPR's one-stop-shop model working, and what might need to change?

For companies, the one-stop-shop has already paid off. Where previously they had to comply with many different national laws and their interpretations and specifications of the individual supervisory authorities, today it is sufficient to coordinate with the authority at the European headquarters.

However, this coordination effort has not been eliminated by the GDPR! It has merely been shifted to the supervisory authorities. This means that the national supervisory authorities had to be reorganised and integrated into the network of European data protection supervision. This was an enormous effort. In my authority, too, not only did technical expertise in the new procedures and language skills have to be built up, but far-reaching structural changes to the organisation of the authorities were also necessary. We in Berlin were already very well positioned in the European area before the GDPR and were able to build on this. But other authorities in smaller federal states or even smaller member states have faced far greater challenges.

First published on the *Global Data Review* website, October 2021

Another problem results from the fact that data processing companies are not evenly distributed across the EU either. Some of the largest IT corporations in the world are essentially concentrated in two member states. The supervisory authorities there, as lead authorities, are single points of contact for some of the largest data processors in the world and must coordinate the process between all the relevant supervisory authorities in the EU. A small supervisory authority like the one in Luxembourg can quickly reach its limits.

We have had similar experiences with the Irish supervisory authority, where many large internet companies are based. The GDPR stipulates that the supervisory authority at the head office always makes the first move, ie, submits a draft decision on how data protection violations are to be punished. The first draft decision was submitted by the Irish supervisory authority only two years after the GDPR came into force! We have not been able to see any progress beyond that. The reasons for this can be complex, eg workload, complexity of the cases, but also lack of political will. The GDPR lacks a provision according to which cases are decided on the European level if the relevant supervisory authority does not submit a draft decision within a certain period.

That the system otherwise works well is shown by the example of my authority. During my term of office, we have already submitted a large number of draft decisions, all of which have so far been adopted in agreement with the other European supervisory authorities.

Data covering the first three years of GDPR enforcement showed that appeal courts are regularly altering or striking down some regulators' fines, including Berlin's €14.5 million penalty issued to Deutsche Wohnen in 2019. What are your thoughts on this?

The decision of the Berlin Regional Court regarding the fine against Deutsche Wohnen SE is not yet legally binding and a final decision is still pending.

In terms of legal history, the General Data Protection Regulation is a very recent piece of legislation and it is precisely the new data protection

First published on the *Global Data Review* website, October 2021

regulations that have resulted in a number of changes in sanctions practice. For the first time, the supervisory authorities of the member states are directly authorised on the basis of a European law to impose fines in an amount that can also cause large companies to comply with the data protection rules. Accordingly, the German regulations on administrative offences must be interpreted in accordance with the will of the European legislator. We hope that a Supreme Court clarification of the question of the relationship between national law for administrative offences and European data protection law will create the necessary legal certainty.

On the topic of fines, what is your response to criticism of the German calculation scheme, which some lawyers have said produces disproportionately high fines?

With the General Data Protection Regulation, the legislator has determined that fines for data protection violations are to be sanctioned with significantly higher fines in the future.

The German fine concept was developed to meet the requirements of Article 83(1) of the GDPR. Fines must be effective, deterrent and proportionate in individual cases. A deterrent effect through high fines can only be achieved if the imposed amounts cannot be easily paid. In this context, the fine must have a deterrent effect above all with regard to the specific data processing and thus make the unlawful data processing uneconomical in the future in a risk assessment. For this reason, the German concept of fines is based in a first step on the turnover of the company responsible, but also includes the mandatory consideration of the circumstances of the individual case.

The standardisation of the practice of fines in the EU is a declared goal of the GDPR. In Germany alone, there are already 18 sovereign supervisory authorities. Therefore, an important reason for the creation of the fine concept was also to achieve a uniform, transparent and comprehensible application of the legal requirements of the GDPR for the assessment of fines by the German supervisory authorities. Fining concepts in the sanctioning of violations are not uncommon. The German Federal

Financial Supervisory Authority (BaFin) and the German Federal Cartel Office (Bundeskartellamt) also use fine concepts, which the Data Protection Conference [a German body similar to the European Data Protection Board] has used as a guide in developing its fine concept.

Can you tell me anything about how the German regulators' coordinated audit of data transfers to the US after *Schrems* II is going?

The Berlin supervisory authority automatically checked around 900 companies and then wrote to just over 80 companies for which there were indications of inadmissible data exports. Since around 10% of the companies contacted did not initially respond, an information demand notice was issued in these cases. In less than 5% of the companies written to, it turned out that there were actually no data exports.

However, we have not yet completed our review of the responsible parties' responses. In some cases, we were able to determine that responsible parties responded that there would be no data exports, when in fact they were using US service providers. We are not yet able to say how many controllers this affects because the evaluation is not yet complete at this time. In one case, a public company switched from one US service provider to another US service provider after discussions about the inadmissibility of data exports to the US. In another case, communication with the responsible party, the operator of a pharmacy, has so far proved extremely difficult, as the responsible party has since denied the facts – which were initially confirmed and also proven. The few companies that have not, according to their own statements, terminated the data exports are currently being checked again in more detail by us and will then be contacted again. A detailed legal discussion has almost always led to the announcement of a voluntary termination of the data exports in the cases processed to date. However, these proceedings have not yet been concluded either.

First published on the *Global Data Review* website, October 2021

What is next for you?

My legal career has come to an end with the end of my term as Commissioner for Data Protection and Freedom of Information. In the future, I would like to devote more time to my artistic interests, particularly my activities as a sculptor. One thing is certain, however: I will always remain strongly connected to the issue of data protection.

First published on the *Global Data Review* website, October 2021