CONFRONTATIONS EUROPE

EUROPEAN DATA PROTECTION SUPERVISOR : DATA PROTECTION AUTHORITY FOR THE EU INSTITUTIONS

WOJCIECH WIEWIÓROWSKI

European Data Protection Supervisor

On July 13th 2023, Wojciech Wiewiórowski, discussed with us European Data Protection Supervisor's role as well as artificial intelligence and the AI Act during an interview with Confrontations Europe[1]. Here is a trancript of these discussions.

♦ To start this interview, could you tell us more about the institution that you manage? What are the European Data Protection Supervisor's missions?

Wojciech Wiewiórowski : The European Data Protection Supervisor (EDPS) serves as the Data Protection Authority for the EU institutions, functioning as an agency. Consequently, our responsibilities can be broadly categorized into three key areas.

Firstly, our primary duty involves overseeing the compliance of EU institutions and agencies with data protection laws. To illustrate this role, let me give you a short example. If you encounter data protection issues in Brussels concerning a shop or hotel, you would typically seek resolution through the Belgian authority. However, if you face a similar problem with the European Council, European Parliament, or any EU agency, regardless of their location in Europe, it is the EDPS that assumes responsibility for addressing such concerns.

Secondly, an integral aspect of our role involves serving as the principal advisor during the legislative process within the European Union. While national authorities provide advisory services to their respective countries, the EDPS takes on this role for the European Parliament, the Council of the European Union, and the Commission whenever they are in the process of drafting or preparing laws.

The third facet of our responsibilities is to act as the Secretariat for the European Data Protection Board. This board is a collective body composed of data protection authorities from across Europe, and we provide the administrative support and coordination necessary for its effective functioning.

♦Could you describe us the main priorities in this body? What are the main issues you have to address as data protection supervisor?

WW : As the Data Protection Authority, a major portion of our work is intricately linked with emerging technologies and novel methods of information processing. However, when we consider the EDPS in its broader role, supervising the EU institutions and law enforcement authorities stands out as one of the most challenging and impactful aspects. This includes our supervisory role over the European Public Prosecutor Office or bodies like Europol and Eurojust as well as our involvement in activities related to the European Union's coordination of external border control, a significant responsibility that includes overseeing the activities of Frontex.

[1] Interview conducted on 13 July by Thomas Dorget

This facet of our work often proves to be both extensive and contentious since it necessitates navigating through the delicate border between conventional data protection concerns and matters pertaining to national security and international affairs.

♦ **Regarding the topic of artificial intelligence, you have already discussed the subject two years ago in previous interview to a famous European newspaper. What would you say are the main threats to data protection coming from the use of artificial intelligence?**

WW : First of all, it is important to note that there has not been any recent groundbreaking revolutions in the realm of artificial intelligence. What happened is that what used to be available to scientists and major tech companies five or six years ago has become widely accessible to everyone as of 2022, marking the democratization of AI.

Solutions like GPT, for instance, existed prior to this year. Discussions about the advantages and disadvantages of large language models, including GPT, had been ongoing since the year 2016.

"What has changed in 2022 was that AI tools were no longer the exclusive domain of major players and researchers."

Instead, they became accessible to the average person, your neighbor, your landlord, or for everyday professional use. While this shift didn't drastically alter the boundaries of what AI could or could not do, it did bring to the forefront a multitude of concerns and challenges, though it may be an overstatement to label them as outright threats.

I will not talk about the singularity or the idea of computers replacing humans; these topics fall beyond the purview of the Data Protection Commissioner. Nevertheless, there are certainly challenges that we need to address.

I believe it is essential to consider a specific set of questions when you embark on dealing with artificial intelligence solutions. The Information Commissioner of the United Kingdom formulated an insightful list of eight fundamental questions earlier this year. These questions pertain to critical aspects, such as determining the lawful basis for data processing, as well as clarifying your role as either the controller or processor within the system.

In parallel, I can say that when the European Union initiated the development of the Artificial Intelligence Act, I had a degree of skepticism. I believed that, from a data protection standpoint, there was not much more to address, as the principles established in the GDPR essentially applied to artificial intelligence solutions. Nevertheless, there were certainly some questions to be explored, such as those pertaining to liability and tort law. While these questions might not be directly tied to data protection, they do offer a valuable approach to assessing the risks associated with AI and determining effective mitigation strategies.

♦ **We often read that the AI Act proposal would could make the EU a global leader for regulation, in terms of data and data protections. How do you feel about this statement? Would you say that?**

WW : I believe that the term "leader" may not be the most appropriate here. If we consider a leader in regulation as the one who regulates the most, it might imply that the European Union's goal is to establish an excessively regulatory system. However, this is not the desired outcome, as it would resemble systems like the Chinese one, which strictly filters external information.

Instead, I would suggest using the word "benchmark." It conveys our idea more accurately. With the AI Act approach, we expect them to justify why they didn't adopt GDPR solutions when crafting their own data protection laws. I believe that the AI Act has the potential to serve as such a benchmark. However, it is essential to recognize that there have been extensive discussions about this regulation in other jurisdictions, with the United States and the UK serving as notable examples.

What sets the European Union apart is that we don't engage in binary debates between two parties or two groups, as you often find in countries like the UK. Instead, we have 27 member states, each with its own perspective. This multiplicity allows us to consider stakeholders' viewpoints from numerous angles. From this standpoint, I believe that Europeans have made significant progress in discussing the potential challenges and their resolutions compared to other jurisdictions. However, I am keenly observing developments in other regions, recognizing that the solutions they adopt may differ from those preferred by the EU.

♦ **A frequent topic of debate revolves around striking the right balance between the level of regulation we wish to impose and the competitiveness of the economic sector associated with artificial intelligence. In the context of safeguarding citizens' personal data while simultaneously enabling the sector to flourish and evolve within the single market, how do you view this equilibrium within the EU, especially concerning the AI Act?**

WW : On one hand, I've been hearing voices that assert none of the existing AI models on the market, given the evolving definition of AI, seem to fully comply with the proposed Artificial Intelligence Act. This echoes a sentiment reminiscent of when data protection laws were introduced in 1995 and then updated in 2016. During those times, there were dire predictions about the potential impact on competitiveness, even though it was evident that these solutions could ultimately contribute to a competitive advantage for certain companies. Therefore, I'd exercise caution in asserting that the impact on competitiveness would be solely negative or extensive. However, I would not dismiss the concerns voiced by the business and research communities, as they merit consideration.

♦To come back to your responsibilities, do you consider that the two crises we experienced in the last four years, namely the COVID pandemic and the conflict in Ukraine, altered the way you approach your responsibilities?

WW : To a certain extent, yes, the past four years have brought changes to my approach. It has highlighted the fundamental importance of privacy and data protection within the European perspective on the world.

In 2020, when the COVID crisis emerged, I had some doubts about its potential impact on privacy and data protection laws. I was concerned that individuals might prioritize security in a very physical sense over privacy. However, I found reassurance in the ongoing discussions about every solution proposed during the COVID crisis, particularly those that touched upon privacy. Privacy and data protection considerations consistently played a significant role in these discussions. What became evident was that both the General Data Protection Regulation (GDPR) and the ePrivacy Directive offered adequate tools for addressing crisis situations.

The interventions required due to the COVID crisis were legally sound under GDPR and privacy regulations. There was no need to modify these laws to introduce specific provisions or special measures. Importantly, all these tools were temporary, and we planned for sunset clauses from the outset, which was reassuring.

Regarding the war in Ukraine, it raised questions concerning the precise nature of the national security exemption in data protection laws. So far, I haven't observed any developments that challenge data protection laws. Instead, what I have witnessed is an expectation that countries like Ukraine, as they align themselves with Western alliances, should also prepare for privacy and data protection challenges. This cooperation has been ongoing and evolving, and I'm pleased to note my involvement as a person of Polish origin.

"When Ukraine established its Data Protection Authority for the first time, it was countries from the former Eastern Bloc, like Poland, that extended a helping hand to Ukraine in adopting a Western perspective on data protection."

♦ Bouncing off the previous example, do you have any discussions on this issue with Moldova, Ukraine, or any kind of non-EU member countries?

WW : Absolutely. It's worth noting that some of the candidate countries, particularly those who have officially initiated the accession process or hold observer status within the European Data Protection Board, have a permanent presence in the board's activities. This includes countries such as Serbia and Albania.

For other nations, our cooperation takes various forms, often aligned with existing frameworks. For instance, they participate in forums like the Council of Europe's spring conference of data protection commissioners. This includes countries like Ukraine and Moldova.

Additionally, we engage in ad hoc actions, such as an upcoming visit by representatives from the Eastern Partnership and Western Balkans that we are organizing in Brussels this September. We also contribute to efforts aimed at assisting Ukraine in the development of its data protection legislation, as exemplified by our involvement in initiatives organized by the Spanish government and Spanish legal experts. The initial phase of this endeavor took place in Warsaw approximately three months ago, with the participation of representatives from the European Data Protection Supervisor (EDPS).

♦ **As the European elections of 2024 are approaching, what are your priorities for the upcoming legislative term? Are you involved in the forthcoming European elections, perhaps in offering guidance to potential candidates or any related activities? Additionally, what key priorities would you emphasize for the next legislative term, particularly from the perspective of the European Data Protection Supervisor (EDPS)?**

WW : Regarding the European elections, our involvement is strictly limited to the technical aspects and does not extend to the political dimension. We exercise caution to avoid taking any actions that could be construed as political.

As a Data Protection Commissioner, I believe that the individual candidate I vote for is not as relevant as the differences in approaches to data protection within and between political parties. Data protection is not confined to a specific political ideology; it's neither left-wing nor right-wing, nor is it squarely in the center. People can champion data protection and privacy from a wide range of political perspectives.

In fact, it's healthier for data protection authorities to remain neutral in political discussions. Therefore, we make an effort to distance ourselves from political debates that occur during European elections. However, we must acknowledge that European elections involve significant personal data processing, not only for the electoral process but also for various forms of promotion. A case in point is Cambridge Analytica, which gained notoriety for its activities related to electoral campaigns. The processing of data for electoral purposes is a crucial aspect of our discussions.

I'd like to highlight that after the previous European elections, the European Data Protection Supervisor issued a reprimand to the European Parliament for one of its actions involving a portal created for the elections. So, while we approach this from a technical and organizational standpoint, it is certainly not devoid of political implications.

As for the upcoming legislature, it is worth noting that these elections are taking place nearly 14 years after the inception of discussions about the General Data Protection Regulation (GDPR). In the next parliament from 2025, there will be very few individuals who recall the GDPR debates within political bodies. For most parliamentarians, GDPR will be an established law that has been in place for years and may even be considered for revision.

My concern is that we might veer too far into reconsidering data protection without remembering that data protection is a fundamental right within the European Union. It constitutes an integral part of the EU's constitutional framework.

♦ **Finally, forwarding on these remarks, would you therefore call the next legislature to be careful about the potential consequences of future revisions of the GDPR ?**

WW : It is a complex matter, and it doesn't have a straightforward answer. Two of the five main principles of data protection, purpose limitation, and data minimization, are openly questioned by certain segments of the industry.

Data minimization and purpose limitation face scrutiny, with some arguing that purpose limitation is a significant constraint, preventing the efficient use of data. The argument goes that by imposing purpose limitation, you risk destroying valuable data that might be needed for unforeseen purposes in the future. This viewpoint suggests that data should not be discarded and should remain available for potential reuse for different purposes. While I may not fully endorse this perspective, I acknowledge the existence of such opinions.