Written answers to the questions issued by Coordinators of the LIBE Committee
Wojciech Rafal Wiewiórowski

1. Could you please describe the reasons of your application for the post and why you consider yourself suitable for it?

When I presented myself to the LIBE Committee in 2014 as a candidate to be the Assistant Supervisor, I explained the values that underpinned my commitment to the safeguarding of fundamental rights in the EU. I grew up in an undemocratic country in a period of great upheaval. I will never forget impact of a surveillance state and martial law on ordinary people: the chilling effect of knowing that your private correspondence and phone calls would be routinely checked by the authorities in the name of ‘security’ and for ‘the good of society’. I appreciate from first-hand experience the preciousness and fragility of individual freedom and dignity.

Now, five years later, those values remain the same. But on top of that I now have invaluable experience of applying these values from a position of leadership of an EU institution. Data protection rules in the EU exist not only to ensure individuals are treated fairly and with respect; they also seek to promote the overall European public interest, especially through building confidence in the integrity of the EU internal market. So it has been a great privilege to seek to give satisfaction to individuals who have cause for complaint against how an EU body has handled their data, and to educate leaders of these bodies to be accountable for their actions - which is a key component of the GDPR and Regulation 2018/1725.

In my career to date, I have worked in the private sector and been involved in data mining and finding correlations between datasets. I have 25 years of engagement with the issues of information management from an academic perspective, but I have also worked for over one decade to apply the principles on the ground in national public service.

In early 2015, in the first 100 days of our mandate, Giovanni Buttarelli and I developed a three-pronged strategy of taking data protection into the digital age, forging global partnerships and opening a new chapter for EU data protection. This has been ideal preparation for me to now take our authority to a new level of leadership, building smart and innovative public administration. I intend to lead by example and harness the synergies available to EDPS with its unique place at the heart of the EU institutional architecture as well as the data protection community. In intend to use this privileged position to help address the societal and technical challenges of the third decade of 21st century. This will be my way of serving the idea of Europe.

Lastly, understanding and explaining the implications of emerging technologies has become a crucial element of the day-to-day functions of the EDPS. Not only in my professional capacity, but also as a parent of two young daughters, who are part of the 21st-century ‘Generation Z’ of digital natives, I am committed to ensuring that the digitisation of society and economy works in the interests of everyone and especially future generations. Under my leadership, EDPS will address not only artificial intelligence or Internet of Things, but also be able to understand what role privacy will play in the age of quantum computing, transhumanism, human-computer interfaces and the ubiquitous storage of data.
2. Could you please describe your vision for the future of the authority you would have
to lead as EDPS, including potential challenges you anticipate and your priorities for
this independent authority.

In my time as a student, I was the Director for IT of the European Law Students’
Association. This inspired in me a vision articulated in the Association’s ‘Philosophy
Statement’: “A just world in which there is a respect for human dignity and cultural
diversity”. This is no mere romantic sentiment; it has been the driving force behind all my
activities, from my initial experience in the private sector and in academia to my service in
public administration both on national and European level. This vision is also the source of my
belief in the European project. I strongly believe that EDPS should contribute to building a just
world. The rule of law and human dignity should be at the centre, remembering always that
we are not protecting the data but the human being concerned by the data. Furthermore, we
should respect cultural diversity of Europeans as well as taking cultural and legal differences
into consideration as we seek global solutions in privacy protection.

**European administration** should be **smart and innovative**. It should be able to adapt new
technologies and business models and use them also to make data protection smarter and
modern. The same way I want the EDPS itself to be smarter: making full use of the latest
technologies, listening to a broad range of stakeholders from industry, civil society and
academia on the ‘best and worst in class’ when it comes to using personal data, instilling a
progressive and dynamic management culture, and valuing and nurturing the diverse talents
of the people who work for the authority. Regulation 2018/1725 has conferred on EDPS a
strong set of powers to enforce but also to engage and educate EU bodies on responsible data
practices in the spirit of accountability. I will use these competences to full effect without fear
or favour but with a clear focus on ensuring the best outcome for the individuals EDPS exists
to protect.

**European law** - not only classic data protection acts but all **acquis communautaire** - should
be a **benchmark** for all new regulations around the world. At the moment the EU holds
considerable influence in the regulation of the digital economy, but we cannot take this
position for granted. If we allow our standards to slip, then countries in the world will
increasingly look to other models, such as China’s or the models that are likely to emerge in
India and the United States over the next five years.

The practical positions of the EDPS will be built on the achievements of my predecessors.
In this sense I propose some **continuity, but we cannot rest on our laurels**. In the words of
Lewis Carroll, “We must run as fast as we can, just to stay in place and if you wish to go
anywhere you must run twice as fast as that”.

I am conscious of the special role of the EDPS within the EDPB, as a member and provider
of the Secretariat, which includes ensuring that the GDPR makes a difference on the ground
in the next five years. As well as supporting the EDPB chair with first-class administrators and
equipment, I will do everything within my competence to help the EDPB succeed in delivering
consistent and robust enforcement of the GDPR throughout the EU.

On a policy level, I will provide this Parliament as well as the Council and Commission,
with informed and objective advice on how to respond to the biggest challenges of the coming
years, including the development and deployment of AI systems, biometrics and facial
recognition, blockchain and quantum computing and encryption techniques – for all of which
data protection rules can and should provide important guidance.
3. How do you intend to fulfil the role that the EDPS has been legally attributed regarding the supervision of the JHA agencies and what are your views on exchanges of personal data by and to JHA agencies, specifically regarding supervision of personal data transfers to third countries?

One of the main challenges of the data protection reform in the European Union in recent years has been to restructure the myriad of supervision systems in the EU’s former ‘Third Pillar’. The EU legislator has achieved further convergence of provisions on transfers of data for law enforcement purposes by JHA agencies (with Chapter V of the Law Enforcement Directive, Chapter IX of Regulation 2018/1725, Article 25 of the Europol Regulation, Articles 56-59 of the Eurojust Regulation). I have always argued in favour of further consistency of those provisions. But I have also called for allowing some flexibility, where it is necessary to preserve the separation of powers at national level (especially the independence of the judicial power) or where use of different transfer tools may fulfil specific needs for an agency to exercise its mandate. At the same time, I am mindful of the deadline of 30 April 2022 for the review of the relevant legislation set out in Article 98 of Regulation 2018/1725. I am of the opinion that our goal should be to unify this multiplicity of approaches, if possible and respecting the special circumstances of each instance.

The EDPS has several tools at its disposal for the supervision of JHA agencies and for providing advice to the legislator on their processing activities. Being responsible for supervision and enforcement in EDPS last four years, I have been able to test all of these tools, including advice, recommendations and their rigorous enforcement, not excluding, where necessary, banning the operations which lack the proper legal basis. Similar rules will play an essential role in supervision of EU institutions such as Eurojust or the EPPO. In practice EDPS actions concerning Europol do not differ too much from the other JHA agencies. I would therefore like to serve as a supervisor of JHA agencies, addressing calls for interoperability of systems and transfers of personal data by those agencies to third countries. In particular I propose to focus on:

a) The legislative consultations under Article 42 Regulation 2018/1725:

(1) an institutional safeguard to ensure compliance with Article 16 TFEU and Articles 7 and 8 of the Charter, including for international agreements for transfer of data for law enforcement purposes (see EDPS Opinion 2/2018 on transfer of Europol data for MENA countries);

(2) a tool to promote consistency of data protection provisions in the various EU legal acts, including for provisions on personal data transfers to third countries,

b) Supervision and enforcement of the implementation in practice of the data protection rules by EU institutions, bodies and agencies;

c) The participation of the EDPS in the work of the European Data Protection Board tasked to ensure consistent application of the EU data protection rules, not only with GDPR but also the Law Enforcement Directive.

The latter is particularly relevant since JHA Agencies receive most of their operational personal data from national competent authorities, which are subject to the Law Enforcement Directive. So far, the work of the EDPB in this area has been limited. Under my leadership, the EDPS will continue to push for further guidance on the Law Enforcement Directive for law enforcement authorities.