European Parliament

2019 - 2024

Committee on Civil Liberties, Justice and Home Affairs

Monday, 25 November 2019, 19:00 - 22:30
at the European Parliament
STRASBOURG

Hearing of candidate Mr Yann PADOVA

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

My career has given me **an exhaustive understanding of data protection**, an area I've been working in **for the last 20 years**. I first approached it from the legislator's point of view, in the National Assembly, where I was involved in transposing Directive (EU) No 95/46 into national law and also in drawing up various other draft laws, including a bill establishing a tracking file for sex offenders. It was in the National Assembly, as an **administrator** bound by an obligation of **strict impartiality**, that I learned how to work with elected representatives of **all political stripes** and to negotiate compromise solutions on legislation. I performed the same task with the Commission services when I was working on the first drafts of the General Data Protection Regulation (GDPR). And this **experience of advising the legislator** seems to me particularly relevant for the post of European Supervisor (EDPS) who works with Parliament and the Council.

Later, as Secretary General of the French Data Protection Authority (CNIL), I set up the 'new CNIL' which resulted from the 2004 law and was endowed with new, far-reaching and varied powers. **The CNIL's organisation and procedures have been modified, its powers of enforcement and control placed on a more secure footing, new services and tools have been developed for users,** etc. To explain these new powers, I have launched an ambitious communication policy, including at European level. Given the new tasks assigned to the EDPS, my **experience of introducing change**, of **management**, of implementing new powers, of **rigorous budget management**, of deploying tools and conducting an effective **communication** policy seems to me indispensable for any candidate wishing to perform the role of EDPS successfully.

As Commissioner of the French Energy Regulator (CRE), I oversaw the drafting of the report on data management by energy network operators. The tasks of these network operators are rapidly evolving with the deployment of 'smart grids' and the ensuing collection of data on a massive scale. New opportunities are emerging together with new risks, such as cybercrime. Here too, my experience of building a new regulatory framework in a **strategic industrial sector**, serving the interests of **the end consumer** and promoting **digital trust**, will stand me in good stead as EDPS.

As strategic advisor to **ICO** (the Information Commissioner's Office (UK), **I am currently working on the interface between regulation and innovation**. Since 2016, my role has been to propose the creation of a '**sandbox**' and to support the ICO in this process until its operational deployment. And this debate on innovation for the public good will have to take place at European level, in particular in **Parliament**, given the EU's ambitious plans in the field of AI. The thinking I've done on this subject, as well as my teaching activity and academic publications, will prove useful to me in advising Parliament.

Last but not least, I am currently working as a lawyer in an international law firm. I advise companies in the field of personal data about how to develop innovative projects and governance. The problem of data protection is becoming one of the keys to business competitiveness that will enable some companies to steal a march on others. It also presents greater risks, given the swingeing fines provided for under the GDPR. Today then my task as adviser has becomes more strategic and multi-jurisdictional. **Knowing and understanding what is at stake and how companies work from the inside**, and a familiarity with the constraints upon, and objectives of, their digital transformation, seem to me to be **essential baggage** for anyone aspiring to properly discharge their duties as EDPS.

My varied career path is evidence of my expertise in many different areas, of a strategic vision of the issues involved, of international openness but also of pragmatism. It demonstrates **my ability to build 'bridges'**: **between** different legal **disciplines**, **between law and technology**, between **law and economics**, between the **legal systems of different countries**, between **institutions and leading players**, **including political ones**, **with** interests that **sometimes diverge,** and between **cultures**. It also illustrates my **commitment to the European conception of data protection** and my ability to defend and promote it internationally. This attachment also stems from my **background**. I am half Swedish by my mother, while my father was originally from eastern Poland and I bear the name of an Italian city where my ancestors found refuge.

Finally, I would add that **independence lies at the heart of my professional life.** This was the case when I decided to join the CNIL and the CRE, which are independent authorities. And it remains so today: being a lawyer, I have an ethical obligation to be independent. My record speaks for itself: **my academic articles** on the right to be forgotten, which are in line with the decision of the CJ (C-507/17), and the legal **argument**s I recently deployed **before the CJ** regarding state surveillance (C-511/18) bear this out. Independence is a demanding discipline. It must include a **dialogue with all stakeholders**, otherwise it fosters inaccessibility and aloofness. It is this kind of independence - demanding but **constructive, open but firm** - that the EDPS will need and that I hope to bring to the job so as better **to serve you**.

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?

The rapid development of **artificial intelligence** (AI), self-learning algorithms and the Internet of Things means Europe now faces **unprecedented ethical challenges**. With the volume of data generated doubling every 24 months, how can we regulate algorithms that change themselves and sometimes seem to become independent of their creators? How can we ensure the transparency and intelligibility of these tools that are becoming such a part and parcel of our daily lives? How can we ensure their objectivity and gauge their biases? How can we correct

them when they are show discrimination? These challenges are particularly important as **Europe is caught between two regulatory models:** that of the United States, where there is no horizontal federal data legislation and where it is the judge, or the sectoral regulator, who intervenes after the event; and that of China, characterised by State hypercentralisation of access to data.

In this **geopolitics of data**, in this digital world which is now under construction, Europe **must assert itself** as the new kid on the block. The Commission has announced its intention to submit a proposal on AI within 100 days. And Europe **has the means to realise its ambitions** because it already has a robust legal framework on which to **base** this new regulation: **the GDPR**. This legislation provides for the relevant principles, such as 'accountability', transparency and people's right not to be the subject of a decision taken solely on the basis of automated processing. By using the GDPR as a basis, Europe can and must **manage to use AI in a manner which is ethically responsible and benefits people and society as a whole.** And in charting this **European, people-centred course for AI, the EDPS** has a crucial role to play **in providing advice** to Parliament and presenting it with pragmatic and innovative **proposals**, **and Parliament** has the wherewithal to ensure that this European approach retains its **democratic** credentials. As far as substance is concerned, we could consider introducing a risk-based approach underpinned by a right to experiment, enhanced mechanisms to ensure certification, adjustment and transparency, or even the traceability of the data and algorithms used (towards a data 'passport'). This is the first major challenge that must also be **addressed at international level. And the EDPS** will have to act as **spokesperson for this European approach.**

The second strategic challenge facing the EDPS comes from **the growing value of data and the complexity and the scalability of the data economy.** If the EDPS is to provide advice that is relevant in a **flexible and proactive** manner, and not just reactively, it is key that he or she should understand the value chain and **identify emerging trends** and new players. In order to do so, the EDPS **will have to** expand operational **cooperation** mechanisms with the European **competition** authorities and the **national data protection authorities** and develop partnerships with research centres in economics, **cybersecurity** and the **sociology** of the uses of technology. But above all, the EDPS will have to boost his or her own capacity for **prospective technological** analysis and intervention by **diversifying the profile of staff, thereby making the office of EDPS more independent.**

I have **experience in building prospective technological analysis capacity**since I created a **laboratory of expertise in the CNIL**, one of the first in Europe, while increasing the share of engineers in the workforce from 3% to 10% over 6 years. Because data protection can no longer function in **silos**. In order to be **relevant and perform the duties of a proactive and multidisciplinary** advisor **for Parliament, the Council and the Commission, the EDPS needs to open up** more and create a focal point around a **new strategic project**. And I pledge to **help launch** this project by consulting **stakeholders** within 6 months of taking office, because **independence** is **not the same as autarky**.

The third challenge concerns the issue of sharing and transferring data between States, including third countries, in fighting crime.

The CJ and Parliament have adopted strong positions on this matter which may serve the EDPS as a basis both in their advisory capacity and in their supervisory role (see Q 3).

The final challenge facing the EDPS stems from his or her **role as supervisory authority for** the EU institutions. The EDPS must be a predictable, fair and credible supervisor. To this end, he or she must continue to encourage compliance by the European institutions, **support them as they become more experienced**, for example by offering them **new** 'accountability' **tools**, such as subcontracting contract models, or self-assessment tools, **practical thematic guides** and in-depth cybersecurity training. The EDPS will also need to increase their own **capacity** to perform checks in situ and inspections of documents which call for **specific skills**. I know this because it was I who **set up the CNIL's inspections service**. Finally, the EDPS will have to **publish an annual control programme and report to Parliament in particular on its implementation.** This is essential for **credibility** of this office both within and outside the Union.

In order to meet these challenges, **the EDPS will need Parliament's full support** to obtain an increase in resources that are still insufficient given the tasks and the challenges that lie ahead.

3. How do you intend to fulfil the role that the EDPS has been legally attributed regarding the supervision of the Justice and Home Affairs 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?

In order to effectively control the data processing of the European Justice and Home Affairs agencies, it is an advantage to **know how the criminal justice system**, the judicial institutions and the law enforcement agencies function. In this respect, my experience in the National Assembly's Law Commission and the CNIL (French Data Protection Authority) seem to me particularly relevant.

At the Law Commission, I was in charge of criminal law, monitoring the budget of the prison administration and personal data law. In this context, I worked on all criminal legislation for seven years, including the creation of a database and monitoring arrangements for serious sex offenders (the 'FIJAIS' Digital record for sexual offenders).

As for the CNIL, it was for a long time one of the only data protection agencies in Europe to have ex-ante and ex-post control powers over police and judicial files. That is why, as Secretary General, I organised, in 2008 and 2009, the **first general inspection of the judicial police files** (the 'STIC'), placed under the authority of the competent public prosecutors. At the time of these checks, the STIC held data on 36 million people. This inspection lasted more than a year, involved 19 on-site inspections, the despatch of questionnaires to 34 courts representing 50% of penal activities carried out in France as well as technical queries on security measures and the traceability of data connections. In addition, the right of access of individuals to police data processing files could only be exercised 'indirectly', i.e. the CNIL exercised this right in the name of the applicant; incidentally, the EDPS is also able to do this, pursuant to Article 84 of Regulation 2018/1725. This **unique experience of supervision and practice of the right of indirect access** (nearly 4 000 requests a year to the CNIL) will stand me in particularly good stead as EDPS.

For the EDPS intervenes in a **complex legal framework** which will evolve during the next term of office. Notwithstanding the adoption of Regulation 2018/1725 and Chapter IX thereof, the EDPS' powers remain patchy because they are based on a number of special legal instruments. This is true of operational data processing carried out by Europol, Eurojust or the

European Public Prosecutor's Office. The EDPS does not have the same powers, as the holder of this office cannot impose an administrative fine or order the suspension of international data flows or issue a warning to the European Public Prosecutor's Office. Nor can the EDPS issue Eurojust or the European Public Prosecutor's Office with a processing ban, unlike Europol.

However, existing legal regimes allow the **EDPS to exercise far-reaching supervision over these agencies, which is absolutely indispensable in view of the risks inherent in the processing** of such data **and the prospect of the interoperability** of some data systems. It is data transfers, especially to third countries, that pose the greatest risks and they therefore need the strictest supervision. In the absence of an adequacy decision by the Commission under Directive 2016/680, the role of the EDPS will be crucial.

This supervision already exists with regard to agreements concluded between the Union and third counties for data transfers by Europol. It will have to continue with unflagging rigour. With regard to Eurojust and the European Public Prosecutor's Office, the supervisor will have to use the supervisory powers invested in him or her to ensure that **data transfers are carried out in compliance with the rules laid down in the applicable regulations and in compliance with the requirements of the CJ.** The risk that the data transmitted may be used for other purposes in third States is a real one and strict supervision is needed in this respect.

In order to **avoid the legal fragmentation** of control regimes and thus a weakening of the level of data protection of persons in this highly sensitive area, Article 98 of Regulation 2018/1725 provides for a 'review clause' (no later than 30 April 2022). This clause calls on the Commission to examine the relevant legal acts, ensure their consistency with Directive 2016/680 and identify any divergences that may have created such legal fragmentation. The role of the EDPS will be crucial here to provide feedback and advise the Commission, the Council and Parliament.

To this end, it seems to me **essential that the EDPS should:** (ii) acquire greater **skills** and have more means available to carry out on-site inspections; (iv) **report** more specifically on its supervisory role and (v) develop dedicated **support and compliance tools** in collaboration with the teams of these agencies.