EDPS

19 September 2022

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Mentor Group
Forum for EU-US Legal Economic Affairs

Speech

Wojciech Wiewiórowski
European Data Protection Supervisor

Dear colleagues,

Let me first thank warmly the Mentor Group for the excellent organisation of this prestigious event and for inviting me.

It is an honour to be here today and to talk to you about privacy, security and sovereignty - a series of interconnected themes that are crucial for global debate, which I take part in as the European Data Protection Supervisor – the data protection regulator for the European Union institutions, bodies and agencies and their main advisor in the field of data and privacy. These subjects occupied a prominent place in my professional life in IT business, academia and public administration...

This debate is not a 'nice-to-have', but a '**must-have**' debate; especially today, with Europe faced again with virtual cyber threats, but also a very real **war of aggression on its territory**.

In these times of uncertainty, data protection authorities, including the European Data Protection Supervisor, need to act as watchdogs and speak out in defence of fundamental values and principles common to all liberal democracies.

Today, I would like to reflect on the **paramount importance of the rights to privacy and to the protection of personal data as fundamental rights of each and every person**. As you know, these rights are enshrined at 'constitutional level' in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, and in many constitutions across the 27 Member States (including my country of origin – Poland). They are expressed in a more detailed way in laws, such as the General Data Protection Regulation (GDPR) and the so-called ePrivacy law and the Law Enforcement Directive.

Privacy and data protection emanate from the deep conviction that the processing of data about living individuals touches the dignity of a person, and therefore should be designed to serve humankind and society as a whole. It should not be reduced to purely mercantile or economic considerations.

The human dignity is at stake.

You should not make the ranking of fundamental rights. Whilst freedom of speech is a pre-condition for democracy, privacy and data protection are pre-conditions for individual autonomy. They are then also inextricably linked with the rule of law and other principles underpinning modern liberal democracies, such as non-discrimination. Excessive collection of personal information and various forms of surveillance, pervasive in our modern societies, pose particular challenges to the rule of law. I will be more precise on that later in my speech.

Amongst the fundamental principles underpinning the right to data protection is the principle of **purpose limitation**. It is interesting to note that it was already present in the 1980 OECD Privacy Guidelines (as purpose specification), as well as in the 1995 EU Data Protection Directive. Honouring data subject's expectations about why their personal data is being collected guarantees transparency, predictability, legal certainty and, ultimately, **data subject's trust**. Specifying the purpose of data processing operations is also a pre-requisite for applying other data quality requirements, including adequacy, relevance, proportionality and accuracy of the data collected and the requirements regarding the period of data retention.

Common to many data protection laws are also limits imposed on the collection and use of personal data, including the principle of **data minimisation** according to which data must be adequate, relevant, and in particular limited to what is necessary in relation to the purpose or purposes for which they are processed. This

means that personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

According to certain studies, and on average, between 60% and 73% of all data within an enterprise goes **unused** for analytics. This suggests widespread non-compliance with the data minimisation principle.

In recent years, we have also witnessed several private sector companies amassing unimaginable wealth, influence, and political power that in the past would only have been associated with nation-States. More often than not, that wealth and power is directly linked to their ability to amass data including personal information at a scale that was never possible before (in clear opposition to the data minimisation principle). **This, in turn, presents governments and parliaments across the world with a challenge on how to exercise their sovereign powers in an area monopolised by private gain imperatives**. In my personal view, **this might be one of the single biggest challenges policymakers face today**, a rule of law challenge, and I am convinced that imposing limits on the volume of data about individuals that these companies are allowed to process is key to solving this challenge.

On a more practical level, data minimisation is also **crucial for data security**. When organisations collect more personal data than necessary (often times not immediately used, but only kept for future ventures), **the chances and severity of potential security incidents increase.**

As a way to 'materialise' the purpose limitation and data minimisation principles, as well as the legal obligation of data protection by design and by default under the GDPR, the EDPS has stressed the centrality of **Privacy Enhancing Technologies (PETs)** to support the implementation of the principle of data protection by design and by default.

The EDPS has been advocating the use of PETs for more than a decade now and has been supporting its use and its privacy engineering through initiatives, such as the Internet Privacy Engineering Network (IPEN).

The EDPB Guidelines on **data protection by design and by default** also make this point very clear: controllers should consider both the volume of personal data, as well as the types, categories and **level of detail** of personal data required for the processing purposes. Their design choices should take into account the increased risks to the principles of integrity and confidentiality, data minimisation and storage limitation when processing personal data, and compare it to the **reduction in risks** when collecting smaller amounts and/or less detailed information about data subjects.

I am well aware of the voices who claim that purpose specification and data minimisation are not feasible in the context of Artificial Intelligence applications. The argument is often made that **it is not possible to predict exactly all the purposes for which data will be used in the future**. It is indeed a complex issue, from both a technical and legal point of view. I have two observations to offer in this respect.

First, there are a number of techniques that organisations can adopt in order to develop AI systems that process **as little personal data as possible**, whilst remaining functional (privacy-preserving methods, differential privacy, use of synthetic data).

Secondly, and more fundamentally, data that might be found as useful later in the process for making predictions **does not mean this data is also necessary**. For example, the processing of data from social media to assess the health risks or the creditworthiness of individuals is unlikely to be a compatible purpose. Controllers

need to assess whether the new processing is compatible with the original purpose for which the data was collected, also taking into account the reasonable expectation of individuals, as well as checking whether it needs to seek further consent from them.

I note with interest that the Federal Trade Commission has recently applied the 'AI disgorgement' remedy also as a response to unexpected and unfair data processing in the context of development. The principles of data minimisation and purpose specification are also prominently present in the recent Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security currently subject to public consultation. This is yet another sign of convergence of regulatory approaches to privacy and data protection in the private sphere on both sides of the Atlantic.

I would like to come back to my earlier point about the data-based power of large companies that has been linked to an increase in phenomena including "fake news", election manipulation" and has been described by Prof. Zuboff as "surveillance capitalism". I see efforts in various jurisdictions to tackle this issue. In the EU, there is a recognition that the GDPR alone will not be sufficient to redress the imbalance of power. New rules have therefore been adopted that target the market power of gatekeepers - in the **Digital Markets Act** (DMA). In turn, the **Digital Services Act** (DSA) imposes certain rules for online intermediary services, including content moderation. These rules will apply alongside **the GDPR** and are expected to be beneficial in addressing or limiting "privacy harms" to citizens.

One striking example of commercial surveillance practices relates to invasive **online-targeted advertising**. In this regard, the EDPS considers that online advertising should be regulated more strictly in favour of less intrusive forms of advertising that do not require constant tracking of user interactions and profiling.

The DSA is already a first step towards this goal, since it lays down a **ban on advertising based on profiling using special categories of data and minor's data**.

In addition, the Proposal for a Regulation on the **transparency and targeting of political advertising**, adopted on 25 November 2021 by the European Commission, would provide rules on political advertising services. Here we clearly see where the regulatory approaches to data protection, consumer protection and competition (or "anti-trust") converge. We encounter a 'State sovereignty' dimension again: the need to minimise risks of undue external interference on political ads, disinformation in the context of elections, etc.).

To conclude, **privacy and data protection are indispensable elements of the discussion on 'sovereignty' and its understanding in 21st century**. If sovereignty is understood as the possibility for people to freely decide its future according to the elementary rules of liberal democracy, including rule of law and respect for fundamental rights, is indispensable.

It is harder to think about a "digital sovereignty" in Westphalian meaning. Also thinking about "data sovereignty" seems to be absurd in a world where data "flow" (or rather "access to data") often knows no borders. But, we find the meaning of "digital sovereignty" when we start to talk about cyber-security – where we have no doubt "our sovereign state" (no matter if it is US, Ukraine or Germany) is under attack. The same way EDPS understands that data generated in the Union is processed according to EU values and laws. This includes reducing dependencies and fostering autonomy of the public administration in the EU, and particularly of the EU institutions, offices, bodies and agencies, who are at the heart of the EU policy making and operations at EU level.

This is how I want to recognise "digital sovereignty" of the European Union. The ability to decide about the digital sphere (rather not "territory") where the values we believe in are protected.

I would like to stress that digital sovereignty **does not necessarily imply that personal data must be stored in a specific geographical region** (data localisation) in all circumstances. Instead of focusing on where data is stored, we should rather focus on the conditions of data processing, including those taking place in Europe. Let me stress in this context that data protection authorities are aware of, and support, the ongoing work on the issue of "government access to privately-held data", including in the context of the Global Privacy Assembly and the OECD.

More than digital sovereignty, I would like to refer to the **digital values leadership**, which is at the core of the EU's ambition to not only be strategically autonomous in digital-driven choices, but also to inspire and promote the same values around the globe.

From this perspective, we look forward to the forthcoming new Trans-Atlantic Data Privacy Framework. The EDPS will work with The EDPS will work with the other data protection authorities of the EU in the European Data Protection Board to ensure high data protection standards in that context.

Thank you very much for your attention.