



*Hague Forum 2 July 2020*

*Wojciech Wiewiórowski's contribution*

Good morning, Ladies and Gentlemen.

Two days ago, I presented the EDPS Strategy for my mandate until 2024. It is entitled “Shaping a safer digital future”.

This strategy is particularly inspired by the reality we are living in in these times. It aims to carry out concrete actions to enable the full potential of digital technologies, in line with EU values, and with a focus on promoting the common good, human dignity and fundamental rights while upholding the rule of law and supporting environmental and social sustainability.

The EDPS has recently achieved an important step in its investigation on the use by EU institutions, offices bodies and agencies of Microsoft's products and services.

Our investigation showed that even when using products of a big service provider like Microsoft, controllers still fail in implementing important data protection obligations, such as the obligation to implement data protection by design and by default. Yes, you heard me right: data protection by design and by default are legal obligations. The GDPR (and in our case the EDPR) converted those *principles* into *legal obligations* which controllers need to be able to demonstrate how they have applied them.

The outcome of this investigation demonstrates that there is indeed a significant scope for improvement in the development of contracts between public administration and the most powerful software developers and online service outsourcers.

This also confirmed by the recent amendments of the agreements concluded between Microsoft and the Dutch Ministry of Justice, and Paul van den Berg will tell us more about that experience.

Also we will hear later from Mario Campolargo how the European Commission subsequently invested a substantial amount of time and resources to renegotiate terms to overcome the product's shortcomings, and to put in place diagnostic data flow control mechanisms.

When using products and services of large scale IT providers, including Microsoft, the same level of protection for individual rights throughout the European Economic Area (EEA) needs to be ensured at all levels.

Our efforts resulted in improved terms and conditions offering increased protection for EU Institutions and transparency for both parties.

That is one of the reasons why I decided to share with you all and the public at large today our principal findings and recommendations.

I would like to stress once again, that having fair and compliant terms and conditions is not just for the sake of respecting the letter of the law. We need to look deeper and uphold the rationale behind the law. Here the ultimate goal is to protect people, not the data.

As the supervisory authorities of the European institutions, bodies, offices and agencies, we are engaged in cooperating with public authorities in the Member States, EU institutions and other international organisations to ensure that contractual arrangements and measures comply with data protection laws.

The first step to this cooperation was the establishment of The Hague Forum for Cloud Contracting last year with the aim to provide a common platform for all interested stakeholders and to “take back control” from IT service providers.

However, we are aware that not all organizations or users can devote such time and resources. The application in real life of the data protection by design and by default obligations cannot wait anymore. We urge service providers to accelerate their transition towards data protection by design and design models. We are already in Year 2 after the GDPR has entered into application.

We will do our part as the EDPS to help that all service providers processing personal data, but especially big tech companies, thoroughly follow it.

However, in the course of today you will see that more needs to be done towards compliance and that stronger cooperation remain essential to achieve better protection of individuals' rights.

The EDPS will continue on this path, with the following four initiatives:

First, we expect that the results of our investigation and your contribution will help improve the data protection compliance of all EU institutions and serve as a benchmark for future deployments of digital products and services, in particular those using cloud infrastructures or those making use of Artificial Intelligence.

Microsoft's product and services were our first verification target because of their widespread for the IT foundational support of EUIs administrative functions (and not only), we will keep our radar tuned on other product and services governing the use of digital services for the institutions. We will carry out investigations and enforce, as necessary.

We will continue to call on EUI and other public administrations in the EU to review their external contracts on digital products, software, services and technology to achieve compliance as required by EU data protection laws. One of our concrete commitments is to reinforce the central role of the controller in relation to processors and sub-processors in EUI, both by raising awareness and, more formally, by providing advice on possible contractual clauses. We will also review terms and safeguards for transfers to third countries. We have already been working in this direction and will strengthen our related advisory and enforcement action.

We believe this can be useful also for controllers under the GDPR, considering that we have similar substantial provisions. EU and national

public administrations in Member States, whose mandate is to serve the public interest, should lead by example and can pave the way also in the private B2B (Business To Business) and B2C (Business to Consumer) sectors.

Second, the EDPS is exploring also how to minimise our own reliance on monopoly providers of communications and software services, to avoid detrimental lock-in and work with other EUI and other public administrations in the EU so they can do the same. We will explore how to deploy free and open source software and solutions offering a high degree of reliability, security and data protection compliance.

Thirdly, the EDPS remains committed to driving positive change outside the EU institutions, in order to ensure maximum benefit for as many people as possible. We see that the consistent and efficient enforcement of the GDPR remains a priority for national data protection authorities (DPAs). However, their resources are sometimes insufficient and there are some discrepancies caused by the different legal frameworks and national procedural laws.

In response to these practical constraints, the EDPS believes that solidarity and reinforced cooperation with the European Data Protection Board (EDPB) and other related actors is key. To accompany DPAs in their work, I have proposed the idea of setting up a Support Pool of Experts within the EDPB. This initiative could provide support to DPAs on complex and resource-demanding cases in a genuine expression of European solidarity and burden sharing.

Fourthly, Europe must uphold its values in the digital world. We do not support the creation of artificial geographical borders, but we do prefer

data being processed by entities sharing European values, including privacy and personal data protection.

As a consequence, we as EDPS are notably interested in policy initiatives to achieve better 'digital sovereignty', where data generated in Europe is converted into value for European companies and individuals, and processed in accordance with European values. I am looking forward to hearing from Pearse O'Donohue, how the EU can shape and lead our transition into a fully digital European economy, in line with our values.

For the EDPS, The Hague Forum will continue to be a privileged exchange "platform", also with a view to raise awareness and a common approach.

There are already positive steps in this direction and through our collective exchanges in The Hague Forum and by reinforcing regulatory cooperation, we aim to ensure that these safeguards and measures apply to all consumers and public authorities living and operating in the EEA.

We need more regulatory cooperation and the active participation of all stakeholders: companies, public administrations, competent authorities in data protection, competition and consumer law as well as users and "data subjects". **United** we can accelerate the change that the GDPR has promised.