Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Intervention

by the Federal Commissioner for Data Protection and Freedom of Information
Prof. Ulrich Kelber

for the EDPS panel

“Regulation of global data flows: a story of the impossible?”

at the **CPDP 2022**

on 23rd May 2022
in Brussels

Dear Ladies and Gentlemen,

dear Woijciech,

Thank you for the invitation and the opportunity to take part in this panel with excellent participants!

I am pleased that today we are talking about the immensely important issue of regulating international data flows.

In the first panel this morning in the Grande Halle on “the future of global data flows”, we have already heard about the importance of this issue and recent developments in other regions of the world.

I would like to contribute to this debate with a brief intervention on the **implementation of the Schrems II ruling** by the **EDPB** and the **national supervisory authorities**.

In addition to that I will also take a look at the work of the **Global Privacy Assembly (GPA)** and the **G7** on the topic of “Data Free Flow with Trust” – *on which Audrey Plonk has just informed from the OECD perspective*

On the implementation of the Schrems II ruling:
With its ruling, the ECJ has posed challenges not only for data controllers and processors, but also for supervisory authorities in the EU. The **complex legal and technical requirements** resulting from the judgment for data transfers to third countries for which there is no

adequacy decision has led to a significant increase in the supervisory and advisory practice of DPAs.

In my **administrative practice**, this effect has become apparent by a significant **increase in complaints** relating to third-country transfers and, in particular – following the termination of the Privacy Shield as a result of the Schrems II ruling – in relation to **data transfers to the United States**.

The **advisory practice** has also become more demanding due to a significant **increase in requests from companies and public authorities**, for example on the use of cloud services or on data transfers in the context of web services, software or website tools.

All data protection authorities in the EU are currently faced with more or less similar cases. It is therefore important to take a **coordinated approach** on legal assessments as well as on enforcement.

At EDPB level, this is mainly achieved by drawing up **guidelines** and **recommendations**. In addition to that, the Board seeks to achieve **coherency in the assessment** of concrete cross-border cases.

In the context of Schrems II, I would like to stress in particular the **recommendations 01/2020** on the so-called **Supplementary Measures**. These recommendations are intended to help exporters to carry out the complex legal assessment of the level of protection in the third country and – depending on the outcome – to take possible

“**additional measures”** to safeguard transferred data, as requested by the ECJ, for example by technical means such as end-to-end encryption.

Together with the **new Standard data protection clauses** by the European Commission from June 2021, these recommendations have made a **significant contribution** to the practical implementation of the requirements of the Schrems II judgment.

However, the current situation cannot be considered satisfactory.

Because – as far as we currently know – the **legal situation in the US** as regards competences by intelligence and security authorities to access personal data for reasons of public security or law enforcement **has not yet substantially changed**. **An essentially equivalent level of protection** within the meaning of the GDPR, thus, can still not be concluded.

However, I **hope** that we will see the **necessary legal changes** in the upcoming **successor scheme for the Privacy Shield**, which has been outlined by Commissioner Jourovà at the beginning of this panel.

This would be an **important signal** beyond the transatlantic relationship. I'll come back to this at a later stage.

In any event, the EDPB will closely examine the new trans-atlantic framework in order to determine whether the possibilities of **governmental access** to personal data are **limited** to what is **absolutely necessary**, and whether the necessary possibilities for **legal**

remedies for EU citizens and an **independent supervisory mechanism** are implemented. These were the decisive criteria in the Schrems II-judgment.

The **EDPB** has not only made important *legal* contributions to the implementation of the Schrems II judgment, but plays an increasingly **important role** in the field of **enforcement**, too.

To give you an example, at the beginning of the year, the EDPB launched its first **coordinated action,** in which the member states DPA's jointly investigate the **use of cloud-services by public authorities.** The issue of data transfers to third countries was one aspect in this investigation.

In addition to that, I would like to mention the work of the so-called **Task Force 101** of the EDPB.

The group was established as a result of 101 complaints from the data protection organisation NOYB. Shortly after the Schrems II ruling, those complaints were submitted to several EU data protection authorities. The Task Force analysed the transfer of personal data in the context of Google and Facebook (now Meta) services with the aim of achieving a consistent assessment of legal and IT-related issues.

I hope that these examples illustrate the role of the EDPB in the implementation of Schrems II. In addition to that, the **DPAs themselves** of course are engaged at national level in implementing the judgement

by advising controllers and take necessary enforcement measures where required.

This **leads me to some remarks** to the **main topic** of our panel, the **regulation of international data flows.**

Here, as a result of the Internet and the digital transformation of our economies and societies, we face the creation of a de facto **global data space**, which – however – is **lacking an underlying regulatory framework.** From a global perspective, the EU with its supranational legal framework is an exception, and it is limited to its Member States.

In order to keep pace with the development of digital trade and technologies, efforts are therefore needed in order to achieve **common legal principles at international level**.

In this context, **international organisations** and **international fora** play an important role.

Let me just mention

- the **Council of Europe** with its **Data Protection Convention 108**, the first legally binding international instrument in the field of data protection, with 55 parties to the convention, modernized in 2018 (“Convention 108+”),
- the **OECD** with its **Privacy-Guidelines** and other important work in the context of interoperability and DFFT,

- and, for the Asia-Pacific Region, the **APEC Global Cross-Border Privacy System (CBPR)** with currently 9 participating economies (Australia, Canada, Taiwan, Japan, Mexico, Singapore, South Korea, the Philippines, and USA).

In addition to these fora, I would also like to mention the **Global Privacy Assembly (GPA)** and the **G7**.

The **GPA** can be an important **multiplier**. As a group of data protection and privacy authorities comprising 130 members from all regions of the world, it is a global forum where different approaches are being discussed with the aim of achieving common views.

The group is not an international organisation, it therefore cannot itself adopt binding rules; however, its members can advise parliaments and governments on cross-border issues and possible legal paths to take to achieve interoperability and trustworthiness in global data flows.

As an example, the GPA at its recent conference last October adopted an important **Resolution on Government Access to Data** (*Resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes).*

Let me **finally** talk about the **German G7 presidency.**

Following up the G7 presidency of the United Kingdom last year, the German presidency has continued the dialogue on **Data Free Flow with Trust (DFFT)** in the **G7 Digital Minister Track** and discussed it as a central topic in the **context of international data spaces.**

I very much **welcome** the commitment of the G7 Digital Ministers to **democratic values in international data flows** in their declaration of 11 May!

The **"Action Plan for Promoting Data Free Flow with Trust"**, which was adopted simultaneously, also provides to continue the **dialogue between policy makers and the G7 data protection and privacy authorities.** We will comply with this expectation this year at the **G7 DPA Roundtable in September**, hosted by me.

It is now important to **further advance at international level the idea of DFFT** with the aim of a common understanding of the underlying legal and democratic principles for secure and trustworthy data flows in a global digital economy.

At the **conclusion** of my intervention, let me come back to Schrems II:

Should it actually come to substantial legal changes in the US, which will be the basis for a new — hopefully this time legally compliant — adequacy decision by the European Commission, the non-EU G7 countries USA, UK, Canada, Japan would be regarded as having a level of data protection **essentially equivalent** to the level of protection under

EU law. Because in this case, for all non-EU G7 countries, EU adequacy decisions would exist.

This would *de facto* create a **G7 data space** within which data transfers could take place without prior authorisation or complex assessments of "supplementary measures".

However, despite the positive effect of such a possible development, we have to consider that this approach would be **limited to the G7**. In other regions of the world, alternative systems to EU adequacy and GDPR transfer tools have been developed.

This is in particular true for the **Global Cross-Border Privacy Rules (CBPR) Forum**, which has recently been announced by the USA, Canada and Japan, together with 4 other APEC countries (Rep. of Korea, Philippines, Singapore, Chinese Taipei). The aim of the Forum is to build on the **APEC CBPR Certification** a make it a self-standing **global certification scheme to facilitate trade and international data flows**.

Given the obvious **differences** at hand between a **supranational legal order** based on fundamental rights – like the GDPR and adequacy decisions based on it – and a **voluntary, certification scheme** based on agreed standards – like the CBPR Certification system – I am sceptical whether the latter approach is sufficient to achieve real trust in international data flows, let alone meeting the high standards of the European Court of Justice.

Coming back to the **title of this panel**: I would not sign that the regulation of global data flows is a “story of the impossible”. But what seems to be the case is that there is still much work ahead of us to come to common ground.

Thank you for your attention!