Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Presentation

of the Federal Commissioner for Data Protection and Freedom of Information

Prof. Ulrich Kelber

# “International data transfers and the need for international harmonisation”

for the online discussion
at the British-German Association

Videoconference on 8 March 2022

Check against delivery

Ladies and Gentlemen,

dear Dr Ni Loideain,

Despite the current sad and disturbing circumstances, I am pleased to be able to exchange opinions with you today, amongst others on the subject of international data transfers.

## I. Introduction

**As we all know, data transfers do not stop at borders**. As a result of the digitalisation of all economic and social sectors, personal data are increasingly transferred and processed globally within the framework of digital services and business models. As this significantly affects personal data, the question arises how these data can be effectively protected during their "journey" through different countries with different legal traditions and thus also different data protection laws.

Data protection is therefore no longer a mere national or European issue, but a **global issue**. The withdrawal of the United Kingdom from the European Union illustrates this fact: Where recently a single judicial area to which the United Kingdom belonged was still in force — the European Union where the GDPR is applicable — national laws now apply and from an EU perspective, the UK is a so-called "third country".

It was therefore necessary to put data transfers between the EU and the UK on a new legal basis, which was realised by the European Commission's adequacy decisions of June 2021. This example illustrates the importance of working internationally to achieve a uniform understanding of the protection of fundamental rights and thus also uniform data protection standards.

The GDPR is a set of rules with a spill-over effect beyond the EU. This is shown by the international developments in Japan and Brazil, where new data protection laws have been adopted and where the GDPR was taken as a model. Korea has also moved closer to EU law, while Mexico, India, South Africa, and even some US States are on a similar path.

However, the GDPR is not only a model for national data protection laws throughout the world; its practical application also extends beyond the borders of the EU and the EEA. On the one hand, this is achieved through the so-called market location or targeting principle in Article 3 paragraph 2 of the GDPR, which applies to data processing by controllers not established in the EU. On the other hand, this is realised through the instruments for transfers to third countries under Chapter V of the GDPR, in particular by means of the European Commission's adequacy decisions, but also through other transfer instruments referred to in Article 46, such as standard contractual clauses (SCCs).

**Even before leaving the EU, Great Britain had already implemented the GDPR into its law and thus incorporated the level of protection provided by the GDPR into its national law**. And I very much hope — and please forgive me for being so frank — that the level of data protection will continue to be equivalent to that of the European Union and that the UK Government will not shake these foundations. Unfortunately, some of the comments made by the British Digital Minister last year give me serious doubts. The consequences would be disastrous for both sides.

However, in this context, I am entirely convinced that a high level of data protection comparable to the GDPR does not necessarily mean to be an obstacle for the British Government pursuing the aim of developing global partnerships quickly and creatively in order to make it easier for British companies to exchange data with important markets and fast-growing national economies.

It is important that the level of data protection in these partnerships reaches a corresponding level comparable to that of the GDPR.

In a globally interconnected world, there must be **free, secure and trustworthy data flows,** regardless of the differences in national and regional jurisdictions. Otherwise, trust in digital transformation, digital services and business models will be lost or will not emerge in the first place. That is why we are also working beyond the European level with international data protection supervisory authorities in order to achieve a high level of protection. However, it is primarily the responsibility of national governments to create the necessary international legal bases. In this context, there are important impulses above all from the OECD and the G7 countries, which are debated under the **heading "Data Free Flow with Trust" (DFFT**).

At this point, I would like to give you a brief overview on the international committees in which we work — mostly together with colleagues from the United Kingdom.

## II. The GPA

This happens, for example, within the framework of the **Global Privacy Assembly (GPA)**. The GPA sees itself as a priority forum for data protection supervisory authorities from all over the world for the purpose of exchanging experiences and for joint consultation on important globally relevant issues. To this end, the GPA can adopt resolutions.

The programme of the Annual Conference 2021 once again demonstrated the importance of international data transfers also in this forum: Several program items were dedicated to this topic. This involved, for example, transfer tools from the different regions of the world. But quite different approaches to solutions have also been addressed, e.g. the **Council of Europe Convention 108+**, updated a few years ago and functioning as the first and only genuine international agreement on data protection rights so far.

## III. G7 Roundtable

In addition, since last year there has also been an exchange within the newly founded G7 group, which includes the data protection supervisor authorities of the G7 countries. The ICO is also represented at this roundtable and my office works well, closely and gladly with the colleagues of the ICO.

This so-called **G7 roundtable of the data protection authorities** was also launched by the British side, in September of last year (7/8 September 2021) by my former British colleague, Elizabeth Denham, in the context of the G7 presidency of the United Kingdom in 2021. As part of this roundtable, we have agreed on closer cooperation between G7 data protection authorities in the digital age. The first meeting of the group took place under the lead topic **“Data Free Flow with Trust” (DFFT)**.

In that meeting, it became clear that technological developments, innovations and increasingly significant international data transfers must go hand in hand with compliance with high data protection standards.

For this purpose, we do not only need cross-cutting regulatory approaches between data protection authorities and other authorities, such as competition and antitrust authorities. Above all, we need an understanding - from the perspective of fundamental rights protection - of the extent to which accesses by security authorities to data in global communications networks are to be tolerated. In this context, data subjects' rights must always play an important role, **because people's and the economy's trust in new technologies and the global digital economy depend on these rights.**

The results of this first G7 roundtable were summarised in a **communiqué**, which is available on the ICO's website[1] and on my website[2].

**This year, Germany has taken over the G7 presidency**. The G7- data protection authorities' exchange of opinions started in 2021 will continue this year as part of the official G7 programme. I am pleased to be given the chance to bring forward this exchange in my capacity as chairman. The topic **"Data Free Flow with Trust" (DFFT)** remains a central concern, which is to be supplemented by the idea of creating so-called **"data spaces"**.

[1] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/09/g7-data-protection-and-privacy-authorities-meeting-communiqu%C3%A9/

[2] https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2021/15_G7-Datensch%C3%BCtzertreffen.html

I am strongly advocating that personal data can be freely exchanged between companies and institutions in the democratically governed states of the world, in accordance with the respectively applicable national rules, in order to enable economic prosperity, promote scientific exchange and also in order to create a counter-model to China, Russia & Co. The national level of protection does not need to be the same if compliance with the respective essential rules of the game is ensured. But what needs to be adapted is the **protection of citizens from disproportionate government access**. There can be no **free and trustworthy flow of data** between countries if the citizens' legal protection is not guaranteed. From a European point of view, states with an Anglo-Saxon background must take a step towards a more global rule of law.

In the context of **International Data Spaces**, for example in the area of health data, existing data should be shared and used, provided that a high level of data protection is guaranteed which is uniform within the space. However, this can only be achieved by means of harmonised rules based on safe and globally recognised transfer tools focusing on the protection of personality and data subjects' rights. Such data spaces can be a basis for valuable and future-oriented cooperation, and also for a new innovation not limited by any borders. First projects in this direction are already in place, such as the European project Gaia-X, which is supported by the Federal Government[3].

[3] https://www.gaia-x.eu/news/events/gaia-x-summit-2021

In all these efforts, our European regulatory framework — the GDPR — can and should set standards and have a role model effect on other legal systems in third countries.

Why don't we promote what we already have and what is considered a quality feature?

For example, taking as a basis the GDPR, **transfer instruments** developed within the EU, such as **codes of conducts** or **certification schemes**, could set **standards worldwide** and have an impact beyond the European Economic Area. We should aspire and aim at being actively involved in the shaping process. And exactly at this point, I see the similarities with the plans of the British Government and those of my British colleague. It is my objective to discuss these approaches for global transfer tools at the G7 roundtable in September with my international partners and to make a joint contribution to the debate on high international legal standards and uniform, secure data spaces.

In this context, we recognize that the degree of bindingnessof recommendations and resolutions by international committees' is certainly lower than binding EU or international law. Nevertheless, this should not prevent us from continuing intensively the exchange and cooperate at international level.

Therefore, we need a **globally harmonised understanding of technologies, legal standards and administrative practices**, even if the path to it will be lengthy and painstaking due to different traditions and standards. And here I assume that my British colleague shares this view.

## IV. Schrems II

I just want to make a short detour before I get to the United Kingdom's data protection law. The **Schrems II judgment** of the ECJ of July 2020 made us aware of problems and risks for international data transfers. International **data flows are accessed, in particular, by intelligence services and other security authorities**. Here, as I have just said, there must be clear — and preferably internationally harmonised — limits. This has been criticised by the European Data Protection Board also in its opinions on the European Commission's adequacy decisions on the United Kingdom, also with regard to the United Kingdom's security laws.

The conclusion which the European Data Protection Authorities and the Commission drew from the judgement is that an adequate level of data protection does not exist in a third country when the access rights of the security authorities are disproportionate. The proportionate design of such access rights, including sufficient rights and legal remedies for data subjects, must therefore become an objective for global transfer standards.

## V. Chapter V GDPR/Adequacy UK

In **Chapter V,** the General Data Protection Regulation provides **a wide range of tools for transfers to a third country** that allow data transfers without any specific authorisation – provided that they comply with the requirements of the ECJ in the Schrems II judgment.

These tools include, inter alia, adequacy decisions, standard data protection clauses, certifications, codes of conducts or Binding Corporate Rules (so-called BCR), but also administrative arrangements. All these transfer tools can set worldwide standards.

From the point of view of the European data protection supervisory authorities, it should therefore be our concern **to promote these transfer tools at international level**.

**Following the Brexit, the United Kingdom is now also a third country within the meaning of Chapter V of the GDPR**.

Consequently, in June 2021, **two adequacy decisions for the United Kingdom** were adopted[4] by the European Commission.

[4] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Both decisions attest, building among others on the current British data protection laws, that the United Kingdom has an essentially equivalent level of protection to that guaranteed under EU law. On this basis, international data transfers to the United Kingdom can take place without the requirement of separate authorisation.

However, almost a year ago, the European Data Protection Board gave a very critical follow-up to the procedure. I would like to pick out only a few points from the EDPB opinion of 13 April 2021 on the adequacy decision having regard to the General Data Protection[5] Regulation.

The EDPB has noted, among other things, that it will be one of the Commission's most important tasks to **monitor the development of the British legal system in the field of data protection as a whole**, because – as briefly mentioned above, the announcements by the UK Government saying that it is intended to develop a separate and independent data protection policy, which could potentially deviate from EU data protection law, have already cast their shadows in advance when the adequacy decisions were adopted[6].

[5] https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf

[6] https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare

The EDPB has specifically requested the Commission to carry out this monitoring. Deviations that pose a risk to maintaining the confirmed adequate level of data protection for personal data transferred from the EU would then have consequences.

Moreover, the announcements made by the United Kingdom Government are also a reason why the adequacy decisions provide for **a four-year sunset clause**. The decision on adequacy ends on 27 June 2025. Until now, adequacy decisions have not generally been accompanied by such a clause. In my view, the UK would lose significantly more than it can win if it amended its data protection law in such a way that the adequacy decisions would not be extended.

The EDPB has also pointed out that it is concerned about the exchange of information and disclosure on the basis of other instruments, such as international agreements, which the United Kingdom has concluded with other third countries. These include, for example, the so-called “UK-US CLOUD Act Agreement”[7] and the “UK-US Communication Intelligence Agreement”. Such arrangements or agreements can circumvent the introduced safeguard measures. This is particularly difficult where, as in the latter example, the arrangement or agreement is not publicly available. It could well be said that in this context, it is an “adequacy decision on probation”. And please forgive me for an assessment that I often provide concerning national security laws: Notwithstanding the requirement for data processing by security authorities, there is often no evidence that the collection of personal data without any reasonable cause really makes a contribution to security. There are rarely figures on this issue, but if you are interested in it, you can look at the utter disproportionateness, for which the monitoring of passenger data serves as an example.

7 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

In addition, the EDPB has called for further clarification and evaluation concerning bulk queries, in particular with regard to the selection and application of selectors, because it is an unresolved question when access to personal data reaches the threshold set by the ECJ and what safeguards are provided for in order to protect the fundamental rights of individuals. The EDPB has asked the European Commission to closely monitor these developments.

It will therefore remain to be seen whether the UK will maintain the appropriate level of data protection currently in place. Let us please call on the British Government, jointly with the EU, to promote a global agreement between democratically governed countries and not to compromise the free flow of data with the EU.

## VI. Conclusion

We should consider the digital transformation, global networking and associated international data exchanges as a great opportunity, as a computer scientist I cannot do otherwise than seeing it this way. But we also need to look at risks and reduce them. The protection of personal data is a fundamental right and also applies in the digital world. Therefore, the following principle shall apply: Digital technologies and business models must be aligned with fundamental rights and not the other way round. This system of values should also apply in the international context, at least between the democratically governed countries of this world.

Particularly the current political situation shows us how vulnerable systems, structures and technologies are to abuse. It also shows us once again that regimes and dictators do not refrain from violating human rights, but use technical means to spread disinformation and track and prosecute people.

Therefore, it is my personal wish that Germany and the United Kingdom will jointly advocate maintaining a fundamental rights- and value-based legal system, and that they will jointly stand up for ensuring a high level of data protection in the digital and global age.

Thank you very much for your attention.