Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Lecture

of the Federal Commissioner for Data Protection
and Freedom of Information

Prof. Ulrich Kelber

“The use of cloud solutions and other services in the context of Schrems II/ the CLOUD Act”

at the Bitkom Privacy Conference
28/09/2022

Online

The spoken word prevails

Dear Ladies and Gentlemen,

I. Introduction

I am delighted to be part of this event today and to see that such a large number of data protection and IT experts from Germany, Europe and around the world come together to discuss important privacy issues.

In the programme, you have already seen the topic of my keynote, with which I will contribute to the discussion today: The use of cloud solutions and other services in the context of Schrems II/ the CLOUD Act. And I claim this title alone contains a whole series of terms like “cloud solutions”, “Schrems II” and “CLOUD Act”, which are at the very beginning capable of triggering a large number of listeners and thus hopefully promoting the objective of a lively and constructive discussion of this topic.

We all see: Data transfers do not know any borders. As a result of the digitisation of all economic and social areas of life, personal data are increasingly being transferred and processed globally in the context of digital services and business models.

As this has a very significant impact from a data protection point of view, the question arises as to how we can deal with these challenges. And you all know that, I don't ask this question for the first time today, it has been asked from many perspectives in recent years and decades, and

lastly dealt with in particular in the context of the title-giving Schrems II judgment and in the context of the CLOUD Act.

Of course, first of all, the question arises as to whether at all and if so how the current data protection challenges following the rulings of the European Court of Justice (ECJ) make further cooperation with US cloud providers possible. This is, without a doubt, not easy to answer at this time and to anticipate the conclusion, no — there is no patent solution that I could present to you here today.

What I can do, however, is to show you the current developments in the handling of cloud services and to identify the requirements that are absolutely necessary from the data protection point of view.

We all agree that the existing uncertainties cannot satisfy all of us. And I am well aware of the worries and needs that arise for the economy from this uncertainty. I take these concerns very seriously, but at the same time I also see it as an opportunity for us to be forced by recent judgments to shape the legal framework in a manner that renders it even clearer and cleaner and thus to exert a targeted influence in order to create data protection-compliant solutions that enable secure and trustful data transfers for all parties involved.

The developments in recent years have shown that data protection “Made in Europe” can certainly become a competitive advantage and this also applies and perhaps even especially in the field of cloud solutions.

Let me explain what I mean in concrete terms and why it is in our interest and must be in our interest that together we create a legally secure and trusting basis for a secure data transfer.

II. Schrems II as a challenge

The consequences of Schrems II are definitely not to be underestimated. International data transfers are now in particular focus again — also in the focus of supervisory authorities. The problem with the use of cloud solutions is that personal data transferred to third countries (such as, but not exclusively, the USA) are treated under legal conditions that do not correspond to the European understanding of an adequate level of data protection that we have committed ourselves to with the introduction of the GDPR. The dilemma can easily be summarised this way.

On 16 July 2020, in its Schrems II judgment, the ECJ declared the EU-US Privacy Shield Decision of the EU Commission null and void. Previously, it was assumed that the requirements of the Privacy Shield largely correspond to the level of data protection of the European Union and thus the transfer of personal data to the USA was possible. In its judgment, the CJEU rejected this assumption.

As a result of the Schrems II decision, data controllers can no longer rely on the adequacy of the level of data protection when transferring data to the United States. This has fundamentally changed the conditions for the transfer of personal.

Notwithstanding that thanks to the Privacy Shield 2.0 (Trans-Atlantic Data Privacy Framework) announced on March 25, 2022, a solution for data transfers to the US begins to emerge, controllers currently still need to rely on Standard Contractual Clauses in particular. For data transfers to the USA and to other third countries, these Standard Contractual Clauses (SCC) are therefore becoming increasingly important as a new legal basis. They contain requirements and contractual obligations intended to safeguard data processing in third countries and to raise them to a level of protection corresponding to that in the EU to some extent. However, the ECJ has already commented on the SCCs in its judgment. Without additional technical and organizational measures, they are usually not sufficient to transfer data to the USA on this basis.

Although SCCs can for the present still be used for data transfers, the mere conclusion of the contract is not yet sufficient for this purpose. Consequently, when transferring data to third countries, companies must check in the end in each individual case whether a level of protection corresponding to the GDPR is guaranteed in the third country. If this is not the case, they must implement additional protective measures and ensure their compliance. There is no question that this is accompanied by a high effort and therefore also with increased costs for companies.

But, and you must not lose sight of this, this is about protecting the fundamental rights of EU citizens.

In June 2021, the European Data Protection Board (EDPB) published new recommendations to help businesses with the “complex task of assessing third countries and identifying appropriate supplementary measures”. These recommendations describe how data exporters — i.e. controllers or processors — can check when processing personal data whether any data transfers to third countries comply with the requirements of the GDPR if there is no European Commission adequacy decision for the third countries concerned. If that is not the case, they provide guidance on how appropriate measures can be taken.

An annex to these recommendations describes use cases where supervisory authorities see possibilities to secure data transfers by means of additional technical measures in such a way that they comply with the requirements of data protection in accordance with Schrems II. In addition, two constellations are presented where, from the supervisory authorities’ point of view, it does not seem possible to take any corresponding measures. On the other hand, this does not mean that in these cases a transfer could not be secured in compliance with data protection — but it will probably be an extreme challenge.

In summary, the following applies: Before transferring personal data to a third country, the data exporter must assess whether an adequate level of data protection can be ensured in the recipient country. And this applies not only to the general level of data protection in the recipient country, but specifically to the data to be transferred. Risks arising from the storage of the data and possible reasonable alternatives must also be examined. If this assessment is negative, thus, if the level of protection is not comparable to the European level, the data exporter must take additional measures before the transfer to guarantee the protection of the data.

Recommended measures include, for example, pseudonymisation, effective encryption, or the choice of a recipient whom the law of the destination country protects against accesses. For providers who have to access data in plain text (e.g. in cloud processing) and to which public authorities have access powers beyond what is necessary for a democratic society, usually no data protection-compliant transfer will be possible.

At this point, it should be pointed out once again as a side note that the problem of transfers to third countries and the responsibility of the controller for the choice of suitable processors does not concern only the USA, but each country without a valid adequacy decision of the EU Commission.

The title of my keynote also refers to the Cloud Act enacted in the U.S. in 2018, which I would like to briefly address at this point in order to make the problem of such data transfers more tangible. Providers of electronic communications or cloud services subject to U.S. law may be required to disclose data under the Cloud Act, regardless of where those data are stored. Therefore, if a US group is in possession of data or has control over data which, for example, are processed in the EU by a subsidiary based in Europe, these data are subject to a potential obligation to disclose them. This makes it clear that European providers, which may fall under the Cloud Act under the circumstances described above, must also be subject to a special audit.

Of course, there are interests justifying the fact that governmental authorities - as part of their work - are also aware of personal data processed by private companies and possibly in other countries. The fight against international terrorism or organised crime are examples of this. However, it always remains decisive under which conditions this takes place, what barriers exist against a boundless data access regime, which procedures of the rule of law are provided for, how the rights of the data subjects are fleshed out and can be enforced. Data protection as a fundamental right also means that all holders of a fundamental right — all persons within the scope of the GDPR — must have the possibility to enforce their fundamental right in court.

The data protection requirements with regard to third country transfers thus remain challenging — especially in the area of cloud solutions.

So yes, it’s complicated. But this example shows what we are protecting with it. The reason for making this effort: To safeguard privacy, not to sacrifice the cornerstones of our democratic values, to reconcile economic success, progress and data protection, thus strengthening our digital sovereignty.

III. Dark clouds above the economy?

Cloud services are the first thing coming to our minds when we talk about Schrems II, but there is also an impact on services that are not directly associated with it, such as in the area of infrastructure.

The cloud market is multi-layered and has become a billion dollar business on which much depends for the economy nowadays. I am aware that due to the narrow stakes set by Schrems II, special constraints have arisen for economic actors. With the above-mentioned recommendations of the EDPB, the supervisory authorities have agreed on this issue and taken initial steps to assist data exporters in the lawful transfer of personal data to third countries. In the preparation of these recommendations, doubts and criticism from stakeholders were taken into account. And we plan to continue doing so. Taking the concerns of the economy seriously, taking up points of criticism and developing the best possible solution for all stakeholders is also our concern.

And that is why I would like to invite you all to continue to engage in this discussion. Let’s not only focus on the difficult starting conditions.

Instead, let’s understand the possibilities that the current situation brings us in order to help shape them as stakeholders. We are open to suggestions from the economy. The framework conditions for international data transfers are now being reorganised — that can be a great opportunity.

IV. A light on the horizon? How is it going on?

To avoid any misunderstanding: It is not about avoiding or even prohibiting third country transfers. It is necessary to find good solutions to the challenges involved, but at the same time, European alternative solutions must be considered. This still proves to be difficult in practice, as there are often no real alternatives to the marketable American cloud providers at the moment. However, it would be desirable that approaches be developed to avoid lock-in effects for non-European suppliers. Though, a comprehensive use of corresponding solutions is not yet apparent.

It is essential that we work not only within Europe, but also beyond Europe on a consistent understanding of data protection. The GDPR is the best example that our efforts are fruitful here. The developments in Japan, Korea or Brazil, where important new data protection laws taking the GDPR as a model have been adopted, show that it is possible to implement good data protection worldwide without economic relations having to suffer. (On this occasion, I cordially greet my colleague Miriam

Wimmer, head of the Brazilian Data Protection Authority, who will report tomorrow on the exciting developments in Brazil.)

In the USA, too, a Privacy Act is being discussed in Parliament at the federal level, just like in India and Argentina and Mexico, and this all happens taking the GDPR into account— there is a lot in motion.

V. A common data space is possible

All this shows that data protection standards should not only be limited to individual countries or international communities, but must be a global concern. On the one hand for the basic rules of governmental access, on the other hand for the general data protection regulations.

A broad common understanding of the protection of fundamental rights and, therefore, data protection must be achieved beyond the borders of Europe so that we can use tools such as cloud solutions in a meaningful and secure manner. This requires international cooperation and cooperative regulatory approaches. In order to be able to create a common data space based on shared values, which allows free movement of data at a high level of protection against governmental access, and in which a wide range of data protection rules for the private sector can then also take effect, all stakeholders must contribute. A common data space that promotes digital innovation, economic

prosperity and a democratic value context would be a gain for all stakeholders at the end of the day.

And in fact, as international data protection supervisory authorities, we are already very active in various formats in order to reach common solutions. Only at the beginning of September in Bonn, at my invitation, we discussed intensively on cross-border data protection and data transfer in the circle of the data protection authorities of the G7 countries.

Such a development would also lead us to globally high data protection standards for private business models, because globally operating companies benefit immensely from unified regulations. The common data space would create a market that differentiates itself from others with data protection-friendly solutions and which makes high data protection standards a key quality feature.

It is important to say that this should not be an exclusive G7/EU-group, but an invitation to states from all over the world. And here I would like to come back to the example of Brazil. Does not the development there show that this idea of a common data space does not have to be a utopia? That we can create common foundations for trusting data transfers in cloud solutions and thus also contribute to economic prosperity. With all the effort — this is a win-win situation for the actors involved.

VI. Cloud and Data Protection

In its judgment, the ECJ made it very clear that the assessment of a data protection-compliant transfer to third countries depends on the specific circumstances of the individual case. As already announced at the beginning: There is no patent solution that I could present to you today.

We — and I actually mean all of us — supervisory authorities, politicians, businesses and civil society must understand it as our shared mission to ensure free, secure and trustworthy data traffic in a globally interconnected world. Clear structures that allow us to protect privacy and democratic values in the best possible way, while combining economic success, digital progress and data protection and strengthening digital sovereignty. Even if it hurts, even if there are no simple solutions.

If we do not achieve this, then we endanger what we are so urgently dependent on: Trust.

If trust in digital transformation, digital services and business models is lost, it will cost us a lot more than the effort and strive we now have to bring up to complete this task to design data protection compliant uses of cloud services. Then the pressure for innovation decreases, consumers have fewer choices, companies are losing ground in international competition.

And that’s why we are working so intensively on a high level of data protection with so many actors beyond the European borders. Creating the necessary legal bases is primarily the task of politicians. With regard to everything going beyond that, such as creating alternatives to marketable vendors and applications, thinking about technical solutions and perhaps sometimes having unconventional ideas in some respects, we can all be involved in. Data protection is not an end in itself, but fundamental rights protection. Data protection is not an obstacle, but, if we design it correctly, a competitive advantage.

Let’s work on it together.

And thank you for your attention.