BfDI Federal Commissioner for Data Protection and Freedom of Information

Lecture

by the Federal Commissioner for Data Protection and Freedom of Information

Prof. Ulrich Kelber

# „The Schrems II ruling oft he ECJ and ist consequences“

at the conference „Data Protection in the Digital Era“ at the University of Istanbul

[online, 16. April 2021]

only the spoken word applies

First of all, I would like to express my sincere thanks for the invitation from the Dean, Prof. Dr. Ekmekçi *[spricht sich: Eckmeckschi].* I was happy to accept. But before I get to my actual topic - the implications of the Schrems II ruling by the European Court of Justice - I would like to preface my remarks with a few brief sentences on data protection in general.

In my opinion, events such as these are the best proof of the importance of data protection in our everyday lives.

In Germany and the European Union, data protection even has constitutional status, but even beyond this nucleus of modern data protection law, more and more countries around the world are recognizing how important it is to protect the elementary legal interests of their citizens through a functioning data protection system.

As data transfers today are no longer local, but for the most part global, data protection cannot be limited just to the legal systems of individual countries but rather has to be seen as a “global undertaking”. This is precisely why it is good and important to regularly look beyond one's national horizons and exchange ideas with colleagues from other countries.

Consequently, official bodies such as the European Data Protection Conference or the Global Privacy Assembly, both of which my Turkish colleague Prof. Dr. Bilir [Präsident der türkischen Datenschutzbehörde, der ebenfalls an der Veranstaltung (mit einem Grußwort zu Beginn) teilnimmt bzw. teilgenommen hat] is also a member, are taking on an increasingly important role when it comes to finding solutions to the challenges that digitization and globalization pose for data protection. However, the exchange of ideas and positions at events such as this is no less important, as this can usually be more direct and thus in many cases more intensive. This is all the more true when meetings can hopefully be held in person again in the near future.

## Introduction

Now to the actual topic of my keynote. The Schrems II decision is a ruling with far-reaching effects, precisely because of the internationalization of data traffic that I already mentioned.

Even though public reporting on the ruling has focused primarily on data transfers from the European Economic Area to the United States, the implications go far beyond this. Rather, it made a complete reassessment of all international data transfers to third countries necessary.

## What does the ECJ say in its ruling?

Let's first look at the two key points of the ruling. With both of them, the ECJ comes to far reaching conclusions that have properly shaken up data protection practice for data processors as well as supervisory authorities.

First, it declares the Privacy Shield invalid. Thus, within only five years of its decision on the "Safe Harbour" agreement, the court once again declares an adequacy decision to be inadmissible as a basis for data transfers to the U.S.

What is noteworthy in this context is not so much the fact that one of several possible legal vehicles for data transfers to the U.S. has been eliminated, but the reasoning as to why. Thus, the court found that in the U.S. there is no level of protection for personal data from the EU that is essentially equivalent to their protection under the GDPR interpreted in light of the Charter of Fundamental Rights of the European Union, since precisely the extensive access rights for law enforcement authorities under U.S. law are not secured by adequate measures to protect the rights of the data subjects.

The ECJ then also takes up this finding, specifically related to the situation in the U.S., of the imperative need to guarantee effective legal protection measures in the second main point of its decision.

On the one hand, it states that the standard data protection clauses adopted by the EU Commission can in principle be used as a suitable measure to ensure an appropriate level of protection for data transferred to third countries. In the same breath, it points out that the enforceable rights and remedies contractually agreed to in these clauses must be available in the third country not only on paper, but also in practice through effective mechanisms. For only in this way the protection required by the EU Charter of Fundamental Rights can actually be guaranteed.

In concrete terms, this initially means the following:

The transfer of personal data to the USA is now only possible on the basis of appropriate safeguards under Art. 46 GDPR, such as standard data protection clauses. The relatively convenient recourse to the Privacy Shield mechanism has ceased to be a basis for transfer since the judgment. The court did not provide for a transition period.

Even when switching from the Privacy Shield to standard data protection clauses as basis for data transfers, additional measures must be provided to adequately protect the transferred data from disproportionate access by U.S. law enforcement authorities and intelligence agencies in specific individual cases, since there is no essentially equivalent legal protection for EU citizens against such access in the United States.

Recourse to Art. 49 GDPR, which provides for exceptions in certain cases, is of course still possible. However, due to the explicit design of this provision as an exception, it does not provide as a solution to the problems faced by data controllers since the ruling.

Obligations of the responsible parties arising from the judgment

For responsible data processors this results in significant practical challenges and obligations if they want or even have to transfer personal data to third countries.

First, they must immediately initiate a comprehensive review of potentially affected data transfers in response to the ECJ's guidance.

In doing so, they have to avoid the error of limiting themselves to data transfers to the U.S. due to the specific reference of the ruling. The court's statements on the law enforcement authorities' access in the absence of compensation mechanisms must be applied to all data transfers from the EU to third countries.

The fact that countries such as China or Russia are probably just as unlikely to guarantee the protection requirements of the GDPR, should be beyond question.

It is equally important not to limit the assesment to data transfers from the European Economic Area directly to partners in third countries. Not only paper applications with personal data digitally recorded in a customer center in Chile or access to the customer relations system of a call center outsourced to India must be considered in the audit.

Beyond those “evident” cases, the transfer of personal data that occurs in the context of the use of digital tools must also be taken into account. In fact, a very large part of our digital life takes place at US companies such as Microsoft, Google or Amazon Cloud Services, where data is transmitted to servers in the USA or covered by US law and processed there. Many of these services are by now only offered in the form of or based on software or infrastructure as a service. Here nearly all data is processed “in the cloud”. This makes it impossible for the vast majority of users to prevent even unwanted data transfers.

Once all relevant data transfers have been identified, they must be reviewed to determine whether the currently adopted protection measures under Chapter V of the GDPR in the respective third country provide substantially equivalent protection under the standards of the ECJ ruling.

This is where the next challenge arises, since in this context it must always first be checked whether the law of the recipient country - or in some cases perhaps simply the de facto conditions - permits access to the data by law enforcement authorities and whether this access is adequately safeguarded by appropriate legal protection measures in accordance with the standards of European data protection law.

If this is not the case, the selected protection measures may have to be changed. Additionally it has to be checked whether additional measures for the specific transfer have to be taken in order to adequately protect the data.

The result of this audit and the measures taken must also be documented in a manner that is comprehensible to the data protection supervisory authorities.

If the review comes to the conclusion that a sufficient standard of protection within the meaning of the judgment cannot be ensured, the data transfer must be terminated immediately.

So it is by no means the case - as it is sometimes portrayed - that action only needs to be taken when a supervisory authority believes that data transfers to third countries are not sufficiently protected. Depending on the facts and the situation, the supervisory authorities can range from ordering the suspension of a data transfer to a third country to imposing hefty fines of up to 4% of the annual turnover.

Task of the supervisory authorities from the judgment

This brings me to the consequences of the ruling for data protection supervisory authorities. The ECJ has also shown us what our tasks are in implementing its requirements.

In addition to exercising the supervisory powers provided for in the GDPR in the event of a breach, one of the main tasks of the supervisory authorities is to advise data exporters on the subject of international data transfers.

In order to achieve the greatest possible degree of legal clarity and legal certainty, the European Data Protection Board immediately took actions to deal with the consequences of the ruling.

A specially established task force initially provided FAQs on how to deal with the new situation for the first time last fall.

At the beginning of November, the “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data” were published for public consultation. These recommendations set out in detail the procedure for reviewing third-country data transfers, which I already briefly described.

In addition, the recommendations contain as an annex a non-exhaustive list of examples of measures that could potentially be suitable to compensate for deficits in the level of protection in the recipient country. In addition to technical protection measures such as encryption and pseudonymization, the list also includes approaches that could be implemented through additional contractual measures, such as the obligation to check the legality of disclosure orders issued by law enforcement authorities and to take action against them if necessary.

However, as a disclaimer, it must be made clear that this list of measures can in no way be understood as a whitelist which, when implemented, automatically leads to legally compliant data transfers. As the ECJ itself has made very clear, the assessment of international data transfers fundamentally depends on the specific circumstances of each individual case.

The European Data Protection Board cannot and will not be able to provide the off-the-shelf solution that many data controllers hope for or even explicitly request from the supervisory authorities. Rather, it will be a matter of further defining the boundary conditions for auditing data controllers and regularly supplementing examples that have emerged as

best practice approaches from our supervisory practice.

## Data protection policy discussions and next steps

It certainly is hardly surprising that the EDSA's recommendations did not cause any rejoicing, especially among those responsible in the business community. During the nearly six-week public consultation process, the committee received more than 200 comments, most of which were critical of the paper and called for clearer, more practical guidelines from the supervisory authorities in order to continue to maintain international data traffic after the Schrems II ruling. The European Data Protection Board is currently still busy evaluating this flood of comments.

In addition to participating in the consultation process, many stakeholders have also repeatedly contacted my office bilaterally with suggestions for making it easier to deal with the consequences of the ruling.

A recurring approach in this context is the application of the so-called "risk-based approach" when assessing the adequacy requirements for data transfers in question. According to this approach, the assessment should not be based purely on objective criteria, such as the mere existence of a law enforcement authority's ability to access the transferred data. Rather, subjective factors such as the probability of access should also be taken into account in order to determine the actual risk and thus the de facto level of data protection in the relevant country.

According to this approach, the requirements for additional measures would be significantly reduced, especially for data that, by its very nature, is supposed to rarely or never come into the focus of law enforcement authorities; particularly in cases or areas where disclosure orders so far have never been issued.

However, the European Data Protection Board has yet rejected the application of the risk-based approach. The main reason for this position is that although the GDPR does provide for a corresponding approach in some places, neither the wording of nor its legislative history provide any proof that the legislator saw any room for a risk-based approach in Chapter V, which regulates the transfer of data to third countries.

The recourse to a risk assessment as provided for elsewhere within the scope of the GDPR - for example, in the case of technical organizational measures - does not really make sense, especially in the case of transfers to third countries where the level of protection does not correspond to the GDPR in the first place.

Moreover, recourse to the risk-based approach in the present context could not be derived from the ECJ judgment either.

Only time will tell, how these and other contentious questions and points of discussion arising from the Schrems II decision will ultimately be resolved.

## Close

Ladies and gentlemen, as you can see, the consequences of the Schrems II ruling will probably keep us busy for a long time to come. With its decision, the ECJ has posed major challenges not only to the economy, but also to us as supervisory authorities.

The increased effort involved in assessing the level of data protection in largely unknown legal systems and the conclusions that have to be drawn from this about further measures to safeguard important data transfers, place a burden on all those involved in the process.

Nevertheless, it should not be forgotten that the highest European court has made a decision here to protect essential fundamental rights of European citizens.

We should therefore see the ruling as an opportunity for better protection of personal data outside the European Economic Area as well. Perhaps even as a starting point for making our understanding of data protection as defined in the GDPR known in other regions of the world, in the hope that this will further advance data protection globally.

Thank you for your attention.