Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Lecture

of the Federal Commissioner for Data Protection and Freedom of Information

Prof. Ulrich Kelber

Current data protection issues and international data transfers

at Bitkom Privacy Conference

online, 27 September 2021

Check against delivery

Ladies and Gentlemen,

I. [Introduction]

The pandemic crisis has proven to be a lasting change in our daily lives. But complaining about the many hardships does not help us any further. We should now draw the right and lasting lessons from the crisis. In particular, we need to address and remedy the many serious failings – and these have not only arisen with Corona. By now, the word has spread that digitisation has been woefully neglected in companies, administrations and in the education and health sector. Digitisation has been pushed aside and neglected for far too long as annoying and conflict laden. Now, we are paying the price for all those omissions, because we see that in far too many fields we are lagging behind other countries and regions and are not using opportunities.

At this point, however, I would like to talk not only about past failings. It is even more important for me to convey courage and confidence. I am firmly convinced of this: Data protection will drive digitisation to combine the protection of people and economic success. This will succeed when data protection is transmitted into good products. This is comparable with the relationship between economy and ecology.

II. Protection of fundamental rights in times of crisis

For governments, especially in times of crisis, there is a great temptation – of course always for the good of people and the solution of their problems – to cut back people's fundamental rights in order to develop real or supposed solutions in a very specific way.

This stems from the old misconception of overcoming crises more quickly by authoritarian means.

The pandemic is not over yet. But after 18 months, a first conclusion can be drawn. For me, it's certain: **Even in such a time it makes no sense and there is no justification to operate crisis management while bypassing fundamental rights.**

All measures must always be checked for their **suitability**, for example to detect infections, treat infected persons or prevent new infections.

The planned measures must also be **necessary**. That means, particularly restrictive measures must be subject to specific conditions. And after the end of the crisis, such measures must also be withdrawn.

This is particularly true for highly sensitive **health data**. Their use poses particular risks to the persons concerned. Employers, of course, want to know how healthy – and that means how able to work – their employees are. If the old saying "knowledge is power" is valid, then this applies to the hierarchy of management and its employees. The General Data Protection Regulation therefore protects these sensitive data for good reason in Art. 9 para. 1 of the GDPR.

I don't see any reason at all to change this in principle. But of course, where it is appropriate and necessary, the processing of health data, such as the vaccination and zero status of employees, may also be proportionate. That is why we, the data protection authorities, made politics timely aware of what the appropriate legal basis should look like.

Of course, I also know all the reiterated accusations that data protection was the only fundamental right that has not been limited (wrong!) or that data protection has prevented future-oriented projects to combat pandemics (wrong!)

I can only repeat it again and again: **When assessing the various measures to combat the pandemic, there were no really insoluble problems from a data protection perspective. Not a single appropriate and effective anti-pandemic measure has failed due to the veto of data protection supervision!**

The fact that data protection is still being made a scapegoat against one's better knowledge is unfortunately nothing new. Yesterday data protection was an economic barrier, today it prevents the fight against the pandemic, and tomorrow it will again favour criminals. Sometimes it is ignorance, sometimes you want to put aside an annoying regulation to do things that European values don't allow. And it is more and more often persons who have failed to implement digitisation who try to hide behind the excuse of data protection.

III. Data protection and the international question of power

It is true that the GDPR has achieved a great deal nationally, in Europe and worldwide. However, it seems to be the case that limiting the power of the dominant U.S. technology companies is and will remain the unresolved challenge for a long time. Even the much discussed and exemplary German Corona Warning app is technically dependent on Apple's and Google's smartphone systems.

In the pandemic crisis, the power of these US giants has continued to rise. The GDPR should actually provide a toolbox for the supervisory authorities to protect from this power people's right to self-determination, which is laid down in data protection law.

All European supervisory authorities must therefore finally make better use of the cooperation procedure within the European Data Protection Board which is regulated in the GDPR. The existing procedure must also be filled with life in the case of extensive, fundamental and cross-border procedures. It will be crucial for the data protection authorities of the EU Member States to make effective use of the possibilities offered by the GDPR.

With regard to large international data groups, it is therefore more than annoying that in Europe, it was only possible to decide on **one** of the groups' problematic behaviours in terms of data protection law. This is because the lead supervisory authorities from Ireland and also Luxembourg can/shall/ act or want to act simply too slowly.

If we do not soon achieve to close the legal proceedings - pending for almost three years - against Facebook, Amazon and Co at national level and then within the framework of consultations within the EDPB, we can largely write off the reputation and acceptance of the whole set of rules. The GDPR creates the legal framework. But this framework must also be enforced through concrete action. We, the German supervisory authorities, will continue to put pressure on the European committees for this objective.

Much needs to change especially in the implementation of European data protection law. By the way, in order to be able at all to set limits, cooperation between competition protection offices and data protection offices will also become increasingly important.

We see in the US that there too, the business practices of technology companies is encountering more and more resistance, not least in Congress. Again, arguments relating to competition law play a decisive role.

However, the work of the state and of supervisory authorities alone will not be sufficient. The economy is also called upon to take up the international challenge. Right now, in the crisis, I see a great opportunity for the economy to finally score with data protection-friendly solutions. We will have a market where vendors can put a real weight into the balance.

The market still has too little to offer in order to meet the enormous demand although businesses can score with data protection-friendly solutions on national, European and global markets. People will only trust digital systems that do not spy on them and when, as a consequence of using the systems, no disadvantages or reprisals are to be expected. Transparency and a perceptible influence on data protection are imperative prerequisites to win the support of the population.

IV. International data transfers

Data transfers do not stop at borders. Nor at the EU's external borders. We experience this every day in private or in working life. Because data transfers to other countries or at least to the scope of foreign law are now part of our everyday life. Even if we don't see it at first sight, it still takes place every day.

Be it the use of social media profiles or pages, the storage of photos in the cloud or the use of email services and office applications. Also, the order in a large web shop is often associated with a data transfer beyond the borders. Today, our data are no longer collected, stored and used locally, but globally.

That is why data **protection cannot and must not end at the borders**. The GDPR created a set of rules that ensures this protection within the European Union and the European Economic Area, but also works beyond that area by incorporating the so-called marketplace principle.

However, data protection cannot only be limited to individual countries or to a community of states, but must be **a global concern**. This is precisely why it is important that we look beyond our own noses and have regular exchanges with colleagues at national and international level.

As I said, it is important that we work within Europe and beyond to **ensure that there must be a uniform understanding of the protection of fundamental rights and, therefore, of data protection**.

The fact that the GDPR works and is a good and effective set of rules is shown by international **developments such as Japan and Brazil**, where new data protection laws have been adopted, the example of which is the GDPR.

Not least the **Schrems II judgment** of the CJEU more than a year ago was a real thunderbolt with regard to international data transfers.

The judgment sends a clear message to all of us, and by this I mean not only the supervisory authorities, but, above all, the companies:

There can be no adequate level of data protection in a third country if the data subjects' rights are not protected by adequate safeguards against extensive access rights of security authorities.

However, the judgment also states that not all transfers to third countries are per se inadmissible or impossible. On the contrary, the judgment sets a framework concerning the question whether and to what extent data transfers to third countries can take place through appropriate safeguards within the meaning of the GDPR and, if necessary, through additional appropriate measures (the so-called **supplementary measures**). The judgment also indicates the circumstances to be taken into account in the examination and evaluation.

Once again, it should be recalled that the CJEU itself has made it very clear that the assessment as to whether a transfer to third countries is in compliance with data protection depends on the specific circumstances of the individual case.

Therefore, the European Data Protection Board cannot provide and will not be able to provide even in the future a ready-made solution for the question as to how to deal with the judgment.

At European level - not only after the Schrems II judgment - the **European Data Protection Board** has set itself the task of identifying ways in which data can be transferred in line with data protection law to third countries or to international organisations within the meaning of the GDPR.

In the last year, the EDPB has produced several substantial contributions with regard to the appropriate safeguards required in the event of a transfer to third countries. Several third-country-related papers are also currently being prepared.

In particular, I would like to mention the joint opinion of the European Data Protection Board and the European Data Protection Supervisor on the Commission‘s new **standard data protection clauses**.[1] The standard data protection clauses are intended to set for the first time a standard that can be used throughout Europe for the contract design, which makes it easier for companies to implement the corresponding provisions of the GDPR. The standard data protection clauses (SDCs) already refer to the requirements of the Schrems II case-law.

[1] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

It should be noted that the SDCs alone cannot solve the Schrems II issue and that an audit requirement remains necessary as to whether the personal data are adequately protected on a case-by-case basis when they are transferred to a third country. The German national data protection conference expressly drew attention to this fact in a separate press release.

The recommendations on the **supplementary measures** provide assistance in this audit.

These recommendations on Supplementary Measures[2] as a complement to the transfer tools of Chapter V of the GDPR, adopted by the EDPB in June 2021, are a very important support for assessing and securing international data transfers.

These recommendations aim at assisting data exporters in assessing the level of data protection in third countries, in order to take appropriate additional measures, depending on the level of protection of the third country, in order to achieve the level of protection required by the GDPR.

The recommendations show in six steps how this could be possible through additional measures following an assessment of the transfer and the legal situation in the third country.

In this context I want to clarify again: It is important to always examine the specific individual case.

[2] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

There can therefore also be the result, after an appropriate examination, that a transfer to a third country which is in line with data protection law is not possible at all.

In the future, it will be important to develop the framework conditions for this audit, taking into account best practice approaches from supervisory practice.

Similarly, in July 2021, the **Guidelines on Codes of Conduct were adopted by the EDPB as a transmission tool** [3]. It is the aim of these guidelines that a code of conduct approved by the competent supervisory authority – following the EDPB's opinion - and declared universally valid by the European Commission, may also be used for the processing of personal data by controllers/processors which are not subject to the GDPR. They are addressed to the supervisory authorities, the Commission, but also to users wishing to apply for authorisation. The guidelines are still in the public consultation until 1st October 2021. So there is still the possibility to get involved for a few days.

In addition, the EDPB is working on further guidelines and papers in various expert groups also dealing with international data transfers – for example with regard to the so-called **BCRs (binding corporate rules**), but also concerning a possible **certification as a transfer tool**.

[3] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en

In addition to the revised standard data protection clauses, the **European Commission** also adopted **several adequacy decisions** last year. Among other things, **two adequacy decisions were adopted for the United Kingdom**.[4] After the Brexit, the United Kingdom is now also a third country within the meaning of Chapter V of the GDPR. Although the European Data Protection Board has been critically monitoring the process, this basis on which international data transfers to the UK can take place now is an important and necessary step to achieve an adequate level of data protection. It remains to be seen whether the UK will maintain the level of data protection. This is also why a sunset clause has been included. Political announcements in the UK to expand the so-called legitimate interest of the data processor to an almost unlimited extent constitute a dangerous development.

For **South Korea**, the Commission launched the procedure for adopting an adequacy decision in June. The EDPB has made its opinion on this matter Thursday last week.

However, with regard to adequacy decisions, it is vital to point out that the content of these decisions varies from country to country. This must therefore always be observed on a case-by-case basis.

But not only at European level, data protection supervisory authorities are working on a high level of protection while promoting innovation, growth and competitiveness in the single market for digital services.

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

There is also an exchange at **international level**, such as the **Global Privacy Assembly (GPA**). In addition, there exists now – launched this year – an exchange within the **(new) G7 group**, where also an intensive discussion on international data transfers takes place.

The **Global Privacy Assembly** (GPA) is the former International Conference of Data Protection and Privacy Commissioners (ICDPPC until 2019) whose first meeting took place in Bonn in 1979. 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; for this purpose, the GPA can adopt joint resolutions. The programme of the Annual Conference 2021 once again demonstrates the importance of international data transfers in this forum: Several program items are dedicated to this topic. As a member of the Executive Committee of the GPA, I would like to take the opportunity to draw your attention to this year's digital-only conference, which will be held in Mexico from 18 to 19 October.

It was only at the beginning of September that the **G7 Roundtable of the data protection authorities** (7/8.09.2021) was initiated by my colleague ICO Ms Denham in the context of this year's G 7 Presidency of the UK. At that roundtable, closer cooperation opportunities between the G7 data protection authorities in the digital age were determined and agreed. This year's **main theme** was **"Data Free Flow with Trust"** (DFFT).

In this context, it became clear that technological developments and increasingly important international data transfers must go hand in hand with compliance with high data protection standards. This requires not only cross-cutting regulatory approaches between data protection authorities and other authorities, such as competition authorities and cartel authorities, but also an understanding of the extent to which access by security authorities to data in global communications networks is tolerable from the perspective of fundamental rights protection. This is the decisive factor for the confidence of people and of economic actors in new technologies and in the global digital economy.

Let me personally emphasise that in terms of economic policy, I consider the creation of a common data space between Europe, North America, Japan, Australia, South Korea, India and other democratically governed states to be indispensable. In order to make this legally safe, it must happen at a high common level of data protection. A race to the bottom must not happen. In Europe this would undoubtedly be stopped by the European Court of Justice.

Finally, the topic of international data transfers also takes place at **national level**. Even within the **Data Protection Conference and its working groups**, the Schrems II judgement and thus also international data traffic is a perennial issue.

Of course, supervision is particularly sensitised when it comes to international data transfers. Since June, **the Länder's ["Federal States'"] data protection supervisory authorities have started controls focusing on data transfers by companies to recipients in third countries**.

As regards the Schrems II judgment, these measures aim at achieving a broad enforcement of the requirements of the European Court of Justice.

For my part, I am also preparing appropriate controls for my area of competence. These controls will start soon. In this context, it will not be a question of whether a company or public authority has already achieved to organise all data transfers in such a way that they fully comply with the case-law of the European Court of Justice. But we will look closely at whether any efforts have started and whether the biggest risks have been eliminated.

In conclusion:

Digital innovations, global networking and associated international data exchanges are above all an opportunity. But they also harbour risks and therefore need political and legal support.

The protection of personal data is a fundamental right. Therefore, the principle must apply that digital technologies and business models must be aligned with fundamental rights and not vice versa. The Schrems II judgment reflects the EU’s fundamental rights-based value system. We should understand it as an opportunity and a call to preserve and maintain these values and fundamental rights within and beyond the borders of the EU in the global digital age, which has just begun. This is not only the mission and responsibility of the public authorities, but also of the digital economy itself, which significantly drives and further advances technological development.

Thank you for your attention.