

GUEST EDITORIAL

THE GLOBAL REACH OF EU FUNDAMENTAL RIGHTS. DATA PROTECTION AND THE RIGHT TO AN EFFECTIVE REMEDY

*Herwig C.H. Hofmann**

The CJEU ruling in *Schrems v Data Protection Commissioner (DPC)*¹ will be subject to many discussions on constitutional matters for the time to come. It is a landmark case not only for clarifying and applying the basic conceptual understanding of fundamental rights in the EU. *Schrems v DPC* clarifies therein many further conditions for effective protection of a right, supervision by Member State authorities as well as the global reach of EU fundamental rights. As most essential developments in public law, this case originates from the very specific structural and substantive context of a specific policy area's administrative law details. But the consequences will radiate far into debates on pluralism of multi-level legal orders in an inter-connected world.

* Professor of European and Transnational Public Law, University of Luxembourg

¹ CJEU C-362/14 *Schrems v Data Protection Commissioner* of 6 October 2015, ECLI:EU:C:2015:650. The author represented Maximilian Schrems before the CJEU.

The background to *Schrems v DPC* is as follows: Supervision of compliance with EU data protection rules takes place by national authorities vested with “complete independence”² within the territory of each Member State. Transfer of data from the EU to a third country is possible only if that country has an “adequate level” of data protection, a fact the European Commission may certify by means of a decision.³ In 2000, the Commission had taken an adequacy decision with respect to the United States of America, a decision became known as the “Safe Harbour Decision”.⁴ Upon request for preliminary reference by the High Court of Ireland in a judicial review procedure of a decision of the Irish Data Protection Commissioner (DPC) not to accept a complaint about Facebook Ireland transferring personal data to Facebook servers in the US, the Court of Justice of the European Union (CJEU) had the opportunity to review the compliance of the various elements of the data protection regime, especially the conditions of the Commission decisions declaring a third country to maintain an adequate level of protection.

This case - *Schrems v DPC* - has the potential to become one of the cornerstones of fundamental rights cases in Europe. The CJEU invalidated the Commission Safe Harbour Decision because it violated the essence both of the right to privacy and the protection of personal data as it arises from Articles 7 and 8 of the CFR as well as the essence of the right to an effective judicial remedy under Article 47 CFR.⁵ Finding violation of the essence of a right, protected specifically under Article 52(1) CFR, means that there is no need to enter into a balancing of various limitations under the principle of proportionality. *Schrems v DPC* is the first case in which the CJEU invalidated an act of EU institutions on the

² Article 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

³ Article 25(1), (2) and (6) of Directive 95/46.

⁴ Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215/7.

⁵ CJEU C-362/14 *Schrems v Data Protection Commissioner*, cit. at 1, §§ 94-95.

basis of violation of the hard core of absolutely protected 'essential' elements of a fundamental right. Extending its findings also to the ancillary procedural rights of Article 47 CFR is important for possibilities of holding administrations to account. The Court found the essence of Article 47 CFR to be violated since the Safe Harbour Decision left individuals with no way of independent review of compliance with their substantive rights in the event of the transfer of data to the US and their processing by secret services.

Schrems v DPC would be famous for this alone. But, importantly for the EU's legal system, it also contains a considerations each of which are of high relevance for EU public law more generally.

A first screening of the case brings to light many points, which without doubt, will be discussed in a string of case reviews and throughout the legal debate in the years to come. Here is a small selection.

One is the international dimension of EU fundamental rights protection. Under the EU data protection directive 95/46, the right to data protection has to follow the data also when it is transferred to a third country. Third countries are authorised as recipients only where provisions are made to ensure some minimum protection. This places information rights in the age of an inter-connected world in a very special context. Although not per se extraterritorially applicable, they have to be protected on a global scale – a level of protection which has to include the right to an effective legal remedy to protect rights of access to personal data, and possibilities of rectification or erasure even in the case of transfer of such data outside of the Union.

In view of this, it remains important to find a definition under which conditions a foreign legal system can be regarded to offer adequate protection in view of EU law. Schrems v DPC illustrates that a non-EU country cannot earn the status of 'adequate protection' simply by guaranteeing the essential elements of the Fundamental Rights in question. In an echo of the 'Solange' case law of the *Bundesverfassungsgericht* and the 'Bosphorus' case of the ECtHR, the substantive and procedural

protection offered by the third country must, according to the CJEU be “essentially equivalent” to the EU level⁶ – a standard many EU countries fail to achieve in their national law.⁷ On December 4th the European Court of Human Rights in Strasbourg (ECtHR) confirmed this reading by a judgement of its Grand Chamber (Case Zakharov v Russia, Application no. 47143/06).

Also, *Schrems v DPC* raises important issues regarding the degree of diligence which both national supervisory authorities and the Commission must show to comply with their obligations under the law in review of transfer of data to third countries. The case, therefore is an important reminder of the developing case law of the duty of care and the obligation to reason decisions accordingly.⁸ And in asking the Commission to regularly revisit its own decision especially when there is reason to believe that conditions have changed, *Schrems v DPC* also contains important clarifications in EU administrative law and the exercise of discretionary powers as a whole.

Further, the case raises very important questions regarding the evolution of the relations between national Courts and the CJEU as well as between the CJEU and the ECtHR. Regarding the latter, since national laws empowering secret services of Member States in some cases are no less intrusive than the US Foreign Intelligence Surveillance Act (FISA) was, the ECtHR will take note of the ECJ judgement when it is presented with requests to review the compatibility of such legislation with the ECHR. On the other hand, the CJEU was confronted with a clearly worded statement by the Irish High Court that the findings of the Commission if reviewed by Irish law would be plainly illegal, was also not willing to fall short of those national expectations. To a certain degree, the CJEU in *Schrems v DPC* plays the ball back into the national field, in stating that national authorities under the

⁶ CJEU C-362/14 *Schrems v Data Protection Commissioner* cit. at 1, § 73.

⁷ See e.g. European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (2015/2635(RSP)), P8_TA(2015)0388 with further references.

⁸ CJEU C-362/14 *Schrems v Data Protection Commissioner* cit. at 1, §§ 63, 75-76, 96-97.

principle of effectiveness in the context of the principle of sincere cooperation (Article 4(3) TEU) must have the possibility, especially in the light of Article 8(3) CFR to “engage in legal proceedings” before a national court – but without explaining how.⁹ This requirement thus sets out obligations on the national legal system and is indicative of the cooperative relation which the national supervisory authorities have with the European Commission in a quasi -composite set of enforcement procedures. Whether the developing relations might continue as a ‘race to the top’ with respect to the protection of fundamental rights in the Union remains to be seen.

For private parties around the globe, questions arise to the practical consequences of the case. The world-wide interest in the judgement, if that can be gauged by the press and media reactions, has possibly surpassed any case the CJEU has so far published. Eyes are now not only on the various national data protection supervisory authorities and their possible findings but also on the Commission as to how it will proceed in ongoing international negotiations. The effects of this judgement will be felt in international trade negotiations such as on the TTiP and TISA. But existing agreements such as the EU-US Terrorist Finance Tracking Programme (TFTP) and the already negotiated EU-US framework agreement on the protection of personal data when transferred and processed for law enforcement purposes will have to be reviewed in the light of the findings of the Court in *Schrems v DPC*.

⁹ CJEU C-362/14 *Schrems v Data Protection Commissioner* cit. at 1, § 65.