THE EU’S ATTEMPTS AT SETTING A GLOBAL DATA PROTECTION NORM

Mistale Taylor, 26th November 2015

Data Protection Directive (95/46/EC)

Art. 4 National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
   
   (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State, when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
   
   (b) the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;
   
   (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community (emphasis added).

Data Protection Directive (95/46/EC)

Art. 25 Principles (Art. 26 – derogations)

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. [...]
## Global Trade of Oligonucleotide Drugs

**23-11-2015**

<table>
<thead>
<tr>
<th>Oligonucleotide Type</th>
<th>Importer Country</th>
<th>Exporter Country</th>
<th>Year</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

### Importer Details

- **Name:** Importer Company Name
- **Address:** Importer Company Address
- **Contact Person:** Importer Contact Person

### Exporter Details

- **Name:** Exporter Company Name
- **Address:** Exporter Company Address
- **Contact Person:** Exporter Contact Person

*Note: The table above is a sample of the actual trade data for oligonucleotide drugs. Actual data may vary depending on the specific year and geographic region.*
THE EU’S ATTEMPTS AT SETTING A GLOBAL DATA PROTECTION NORM

Contents

1. Introduction

2. Diverse conceptual approaches to data protection in international instruments

3. In the Data Protection Directive

   Scope of Application: Article 4, DPD

   Adequacy Decisions: Article 25, DPD

   3(a). Reactions to the adequacy standard

   3(b). Direct effects of the adequacy standard

   3(c). Indirect effects of the adequacy standard

4. In recent CJEU jurisprudence

   4(a). Schrems case

5. The struggle between the EU and external actors

6. Conclusion
1. Introduction

The law of one jurisdiction, namely the EU, has become and is becoming the rule in other places for several reasons, including economic ease, accession goals, convenience, regulatory arbitrage and potentially the protection of human rights. This legal diffusion even suggests an overriding data protection norm; however, there is no clear evidence of the existence of such an all-encompassing, widely-accepted norm outside the EU. Indeed, diverse attitudes to data protection and corresponding laws have caused jurisdictional tensions between the EU and third States, most notably the US.

2. Diverse conceptual approaches to data protection in international instruments

Two of the first international instruments regulating data protection, the non-binding FIPs (1973) and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), facilitated global data flows for economic, not human rights, purposes. The Council of Europe Convention 108, (1981), however, focused more on protecting human rights, including the free flow of information, but also, and notably, the right to privacy.1

The original 1973 United States Federal Trade Commission’s Fair Information Practices (FIPs)2 codified widely-accepted practices on maintaining informational privacy in an electronic marketplace.3 The FIPS are simply recommendations. Accordingly, they are not legally enforceable, but have been highly influential on subsequent legal instruments on protecting personal data to enhance the free flow of information. The relevant organisations that drew up the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the 1981 Council of Europe Convention 108 consciously followed and expanded the major principles in the FIPs.4 In view of this, some might argue that the FIPs, being the core of early data protection principles and quickly enshrined in legal instruments, are neither controversial nor contested around the world. In other words, the FIPs could be evidence of a widely-accepted data protection norm. This research argues, however, that the FIPs were more a short set of principles linked to the free flow of information and trade that unsurprisingly influenced subsequent such instruments. Diverse national data protection laws and no existing global data protection instrument confirms that a globally-accepted data protection norm does not exist.

---

2 They have subsequently been updated and are now called the Fair Information Practice Principles.
In terms of diverse conceptual approaches, we can agree that historical experiences, societal values and traditions influence countries’ privacy laws (if any exist at all). The EU Charter consolidated the right to protection of personal data as an autonomous right based on constitutional traditions common to Member States. EU representatives often use fundamental rights rhetoric to promote the Union’s data protection law. Both of these developments highlight its increasing legal importance. We can accept, too, that the EU has the strictest data protection laws, affording a high level of protection to its citizens’ personal data. As such, in the absence of a global data protection norm or a global data protection treaty, the EU has become something of a trend-setter or leader in this area.

3. In the Data Protection Directive

Scope of Application: Article 4, DPD (admits of a degree of external/extraterritorial effect of EU data protection law)

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community. (emphasis added)

Adequacy Decisions: Article 25 (Article 26 – derogations)

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. [...]  

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4. [...]  

3(a). Reactions to the adequacy standard

---

When the Directive was introduced, the concept of reciprocity in the adequacy standard was promoted.\(^6\) Non-EU officials deemed this approach protectionist and suggested it had an undesirable extraterritorial effect.\(^7\) Since then, however, the EU’s approach to data protection has proven largely successful and effective in using legal diffusion to set a high-level data protection norm around the world.\(^8\)

### 3(b). Direct effects of the adequacy standard

A 2013 geopolitical study of the then 101 States with data protection laws demonstrated that European data protection standards “have had far more influence outside Europe than has been realised” and asserted this influence was only increasing.\(^9\) Here, we look at the quantity and reach of influence, and not necessarily the quality or substance of the laws.

- EU Member States
- EEA – data protection laws consistent with DPD
- Adequacy decisions or close to obtaining them
- Ratified CoE Convention 108 and its Additional Protocol, which is roughly at the DPD standard
- Roughly 53/101 \(\rightarrow\) one jurisdiction’s wide sphere of influence
- E.g. US exception – Commission in negotiations (to be discussed using Schrems example below)

The EU’s clear influence on other States’ data protection laws and its open goal to be influential is a key example of a form of the EU (territorially extending its law by) influencing the content of third State law.\(^10\)

### 3(c). Indirect effects of the adequacy standard

The DPD’s adequacy decision clause, as well as its applicable law provisions, directly or indirectly provide for territorial extension of EU data protection law, whereby EU citizens and potentially third State citizens are subject to EU protections. As its regulation is highly influential and many third States have enacted data protection laws to mirror those of the EU’s in order to obtain adequacy decisions, the EU is purposefully extending an EU-level of data protection to citizens of third States.

---


\(^7\) Ibid.

\(^8\) Ibid.


Mistale Taylor Presentation Notes

Whilst this is largely due to trade reasons, as third States would then easily meet the EU’s adequacy standard required for cross-border data flows, this might evolve if the EU views its role as something of a norm-setter, promoting the right to data protection abroad.

4. In recent CJEU jurisprudence

4(a). Schrems case\textsuperscript{11}

Schrems claimed US privacy laws offered no protection from security agencies using EU citizens’ data for mass State surveillance. He also sought to highlight the general failings of the 2000 US-EU Safe Harbour agreement at ensuring EU residents’ data adequate protection when processed in the US. The Safe Harbour agreement purports to ensure that US companies apply EU-level data protection standards, which are more stringent than those in the US, to EU personal data when it is exported to the US. US companies can join the Safe Harbour agreement voluntarily; they then self-certify their compliance with its provisions. It has always been controversial. In March 2014, the European Parliament called for its suspension. The European Commission is currently attempting to renegotiate the agreement.

On 6\textsuperscript{th} October 2015, the CJEU declared the Safe Harbour agreement invalid, in line with the Advocate General’s opinion. The Court ruled that national supervisory authorities may consider whether data transfers to a third State comply with the relevant DPD and EU Charter provisions, even if the European Commission has found that State to provide an adequate level of data protection. Only the CJEU, however, may declare an adequacy decision invalid.

On the Safe Harbour agreement, the Court stated that the US needed to protect EU citizens’ fundamental rights to an “essentially equivalent” degree as in the EU.\textsuperscript{12} This protection is required by the DPD read together with the EU Charter. The Court found that the Safe Harbour agreement did not prevent US authorities from interfering with EU citizens’ fundamental right to data protection, especially as US security and law enforcement requirements overrule protections in the Safe Harbour agreement. For this and other reasons, the Court declared the agreement invalid.

What qualifies as “essentially equivalent”? Is this a higher standard than “adequate”? Would changing the Safe Harbour agreement to better protect EU citizens’ data exemplify norm diffusion? A form of soft law?

5. The struggle between the EU and external actors

\textsuperscript{11} CJEU (GC), Case C-362/14, Maximilian Schrems v Data Protection Commissioner, 6 October 2015.
\textsuperscript{12} Ibid., paras. 73, 74 and 96.
Scott asserts it is erroneous to suggest that the EU strives to export its own norms through the territorial extension of its law.¹³ This research, however, takes the approach that the EU is a norms-setter that sets norms through leading by example, instead of through coercion.¹⁴ The Union is attempting to set a data protection norm, of which no global norm exists. As no such norm exists, external actors are wont to contest the EU’s stringent approach to data protection law. The Union’s domestic law might appear internationally, whilst what appears internationally might also have an effect on the EU domestically: there is a constant struggle with the EU’s attempts at norm setting and external reactions to this.¹⁵

6. Conclusion

As the fundamental right to data protection morphs to carry more weight in the EU, this could amplify the EU’s obligations under fundamental rights law to protect its citizens’ personal data when such data is processed outside EU territory. It is doing this through the soft power and legal diffusion implied in its adequacy decision requirement and resultant negotiations of data transfer agreements. To extrapolate this further, the EU appears to be moving beyond being simply an economic and political union to something closer to a global fundamental rights actor or norm setter, especially in the data protection realm.