2012

The Intricacies of Independence

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner
Brussels Privacy Hub

Christopher Millard
Cloud Legal Project

Dan Jerker B. Svantession
Bond University

Editorial

The intricacies of independence

Christopher Kuner*, Fred H. Cate**, Christopher Millard**, and Dan Jerker B. Svantesson***

In the European Union, compliance with data protection requirements is overseen by public authorities (ie data protection authorities or DPAs), who 'shall act with complete independence in exercising the functions entrusted to them'.[1] Given the growing number of countries around the world that have adopted data protection legislation based on the EU model, the requirement of having an independent data protection authority has spread to other regions as well. This requirement has recently been reinforced by the judgment of the European Court of Justice (ECJ) in the case *Commission v Germany*,[2] where the Court found that the DPAs of the German federal states (*Länder*) were structured so as to be subject to governmental oversight, and that Germany had thus failed to properly implement Article 28(1) of the EU Data Protection Directive.

These developments lead to reflection on the concept of 'independence'. As the ECJ found, the basis for requiring independence is that it helps ensure the effectiveness and reliability of supervision by allowing the authorities to carry out their tasks free from external influence.[3] The experience in Europe shows the need for such regulatory independence, given that governments sometimes have sought to influence the work of the data protection authorities (one such example is the resignation en masse of the entire Greek Data Protection Commission in 2007 for alleged political interference).

However, the issue of independence is more complex than it may seem at first glance. While independence is indeed an indispensable requirement for the work of DPAs, complete and total independence is never possible, or even desirable, on the part of any public authority. Principles of accountability and transparency require that a supervisory authority be answerable for its actions (eg through the possibility of judicial review), and that it be subject to controls in order to ensure its integrity.

There are also different types of independence. The ECJ decision concentrates on legal independence, that is how the DPAs are set up and structured so as to be free of undue governmental influence. However, just as important is independence in terms of financial and personnel resources. Indeed, many European data protection commissioners complain that they have insufficient resources to do their jobs properly (a view supported by a recent study of the European Agency for Fundamental Rights).[4] Indeed, one European DPA even had to shut down its operations for several months toward the end of 2010 because it had completely run out of funds. Some European governments have used structural independence as a 'poisoned chalice', freeing their DPAs from being part of government ministries but also making it clear that from that point the DPA is required to provide for its own budget. It is therefore welcome that the European Commission has taken a broad view of the concept of independence of the DPAs in its current review of the EU data protection framework.[5]

Independence may also be viewed differently in different legal cultures. For instance, one non-EU DPA has stated privately that in its country, being part of a government ministry gives it more 'clout' and results in it being taken more seriously than if it were set up as a free-standing, independent regulatory authority. It may therefore be necessary to consider the complete legal and political structure of a country before determining whether its data protection regulator is independent.

* Editor-in-Chief
** Editor
***Managing Editor

1 EU Directive 95/46/EC, Article 28(1).

2 Case C-518/07 [2010] ECR I-0000.

3 Ibid. para. 25.

4 See European Union Agency for Fundamental Rights, 'Data Protection in the European Union: the Role of National Data Protection Authorities' (2010), <http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf>, at 42, accessed 19 October 2011, finding that eleven out of twenty-seven national data protection authorities in the EU Member States were unable to carry out the entirety of their tasks because of a lack of financial and human resources.

5 See European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', COM(2010) 609 final, 4 November 2010, at 17.

Differing views as to whether regulators in other countries are sufficiently independent have also given rise to political tensions (such as with regard to the independence of public authorities in the United States). Given the problems the EU has had in ensuring independence among its own DPAs, governments in other regions may smile when they are criticized for the supposed lack of independence of their authorities.

The issue of whether entities performing compliance and enforcement functions are 'independent' will have substantial impact on the future data protection landscape around the world. An obvious example of this occurs in the context of review of the EU legal framework, in which the European Commission is certain to pressure the EU Member States to improve implementation of the requirement of DPA independence resulting from the Directive and the ECJ judgment. But considered more broadly, there is a clear link between DPA independence and the impartiality and integrity of compliance and enforcement schemes that go beyond traditional governmental regulatory structures. In an age of shrinking government budgets, and given the growing interest in putting greater compliance responsibilities on both data controllers and data processors by requiring them to be accountable for their processing of personal data, there will likely be increased 'outsourcing' of compliance and enforcement functions to third parties (including, for example, the management of privacy seal programmes; running alternative dispute resolution mechanisms; and operating certification and audit programmes, to name just a few), with appropriate DPA supervision. However, allowing third parties to manage such schemes will only be effective and credible if they too are seen to enjoy a high level of impartiality and independence from both governments and private sector interests.

Like many other concepts in the world of data protection and privacy law, regulatory independence is a more nuanced and complex subject than it may appear. True independence is a multi-faceted concept that goes beyond requiring the DPA to have a particular legal structure. Rather, an evaluation of a number of elements is required, such as being insulated from political influence; having a sufficient budget to do its job properly; and being able to hire sufficient numbers of qualified staff, while at the same time being able to ensure sufficient accountability. Fulfilling all these factors simultaneously is a tall order, but will become increasingly necessary to ensure the legitimacy and credibility of data protection supervision and enforcement in the years ahead.

doi:10.1093/idpl/ipr021
Advance Access Publication 14 November 2011