The Lisbon Treaty and data protection: What's next for Europe's privacy rules?

By Daniel Cooper, Henriette Tielemans, and David Fink of Covington & Burling LLP's Privacy and Data Protection Practice Group

This article originated as a Covington & Burling LLP Privacy & Data Protection Advisory and is reprinted here with permission.

Daniel Cooper

Henriette Tielemans

David Fink

The Lisbon Treaty entered into force on December 1, 2009. This agreement substantially overhauls the EU's legal bases, the Treaty on European Union (TEU), and the Treaty Establishing the European Community (EC Treaty), the latter of which is renamed the Treaty on the Functioning of the European Union (TFEU). While much attention has been given to the Lisbon Treaty's reform of the EU's institutional arrangements, it also alters the legal grounds for legislation in the data protection area in ways that could impact privacy regulation. Below, we describe the key changes and consider the potential effect on Europe's data protection framework.

Data protection under the current treaties

To date, EU data protection laws have been primarily based on provisions in the EC Treaty empowering the EU to legislate in furtherance of the internal market. Both the landmark Data Protection Directive (95/46/EC) and the e-Privacy Directive (2002/58/EC) were promulgated on this basis, and, consequently, they concern both protection of privacy and the free movement of personal data. Two other provisions also play a role. Article 30(1)(b) TEU requires that transfers of law enforcement information be subject to appropriate data protection measures, and this was the principal basis for Framework Decision 2008/977/JHA. In addition, Article 286 EC Treaty provides for the application of data protection rules to the EU Institutions and for the establishment of an independent body to oversee data protection in this context (this led to the creation of the European Data Protection Supervisor).

The new provision on data protection: individual rights and expanded EU authority

The most striking change for data protection under the Lisbon Treaty is a new, prominent provision on the subject—Article 16 TFEU—which replaces and expands on the old Article 286. Article 16 states as follows:

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

What does this mean for data privacy? First, the provision establishes an explicit right to data protection. It appears that this right would be directly applicable to persons, and that they could consequently invoke it in court. The right to data protection is reinforced by the revised Article 6 TEU, which provides that the EU Charter of Fundamental Rights "shall have the same legal value" as the TEU and the TFEU. This would seem to have the effect of incorporating directly into EU law all of the rights in the Charter, including Article 8 on the Protection of Personal Data. Article 8 contains language essentially identical to clause 1 of Article 16 TFEU, and additionally establishes rights to fair processing of personal data, access to such data, and rectification. The Data Protection Directive already provides that Member States should ensure similar protections.

Second, clause 2 of Article 16 establishes a clear basis for the Council and Parliament to regulate the processing of personal data by Member State authorities when carrying out activities that fall within EU law, in addition to the EU Institutions previously covered by Article 286. But the full scope of this clause is not entirely clear. One could interpret the phrase "and the rules relating to the free movement of such data" as granting the Council and Parliament a general right to legislate data protection rules, including for the private sector. This is not, however, the most obvious reading of the text, which instead seems to refer to regulation of the free movement of personal data among public authorities in Europe. Furthermore, there does not appear to be any reason why the EU could not continue to regu-

*See, **Lisbon Treaty,** page 18*

late data protection in the private sector on the basis of internal market provisions.

Finally, the last sentence of clause 2 references a carve-out for data protection rules in the context of the common foreign and security policy. Under Article 39 TEU, the council, alone, is empowered to adopt rules on the processing of personal data by Member States in this area.

The abolition of the pillar structure and its impact on data protection in law enforcement activities

One of the key structural reforms of the Lisbon Treaty—the abolition of the pillar system—could also affect privacy rules. Pre-Lisbon, the EU comprised three legal pillars with separate legal bases for legislative action: (i) "Community" matters; (ii) Common Foreign and Security Policy; and (iii) Police and Judicial Cooperation in Criminal Matters. Crucially, only the council was empowered to adopt legislation in the third pillar on data protection, pursuant to Article 30(1)(b) TEU.

With the elimination of the pillar structure, it appears that any future laws on data protection in the police and judicial context would be based on Article 16 TFEU, where both the council and the Parliament are co-legislators. But some privacy advocates argue that Framework Decision 2008/977/JHA must also be revised—with input from the Parliament—to reflect the co-legislation requirement, or, alternatively, that the Data Protection Directive must be amended to encompass the use of personal data by police and judicial authorities (this would also involve co-legislation by the council and Parliament). Others, however, might argue that a change in the procedure for adopting legislation does not require the re-opening of laws validly adopted under an old procedure. It remains to be seen how this will play out.