Chapter 2
Data Protection in EU Law after Lisbon:
Challenges, Developments, and Limitations

Maria Tzanou
Keele University, UK

ABSTRACT

This chapter provides an analysis of the data protection rules in EU law, focusing on the constitutional and legal developments after the entry into force of the Lisbon Treaty. It examines the jurisprudence of the Court of Justice of the EU on data protection issues, including the recent decisions of the Court on metadata retention and the new right to be forgotten. It concludes with a critical comment on the possibilities and limitations of the EU to provide for effective and comprehensive data protection.

1. INTRODUCTION

The rapid expansion of the Internet, the development of new technologies which make possible the use of big data and the fight against terrorism and serious crime have led to an unprecedented need for exchange of personal data. Data protection in Europe was born out of the concerns raised in the 1970s about the establishment of huge data banks and the increasingly centralized processing of personal data. In the EU, the first data protection legal instrument, the Data Protection Directive was adopted in 1995. Since then data protection has gone a long way culminating to its constitutional recognition as a fundamental right next to privacy in the EU Charter of Fundamental Rights.

The present chapter provides an analysis of the data protection rules in EU law, focusing on the constitutional and legal developments after the entry into force of the Lisbon Treaty. It examines the jurisprudence of the Court of Justice of the EU on data protection issues, including the recent decisions of the Court on metadata retention and the new right to be forgotten. It concludes with a critical comment on the possibilities and limitations of the EU to provide for effective and comprehensive data protection.

DOI: 10.4018/978-1-4666-7381-6.ch002

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

2. THE EU DATA PROTECTION REGIME AFTER THE LISBON TREATY

2.1 The Lisbon Treaty and Constitutional Developments in the EU

In 2004, two failed referendums in France and the Netherlands marked the early end of the ambitious EU Constitutional Treaty (or the Treaty establishing a Constitution for Europe). Not very long after this, the Lisbon Treaty was signed on December 13, 2007 and entered into force on December 1st 2009. The Lisbon Treaty was presented by its authors –the EU Member States- as an amending Treaty of the founding Treaties of the EU that aimed to introduce only an 'incremental change' (Cremona, 2012, p. 40) and not the complete new legal framework that the Constitutional Treaty proposed. However, the Lisbon Treaty represents an important new departure for the EU (Berman, 2012, p. 3) and marked a new era for the EU constitutional and human rights framework in general and the right to data protection in particular.

The pre-Lisbon EU constitutional framework was built-up on the so-called three –pillar system: the first encompassed the European Community (EC) Treaty and Euratom (and formerly the Coal and Steel Community); the second the provisions on Common Foreign and Security Policy (CFSP); and the third the provisions on Police and Judicial Cooperation in Criminal Matters (PJC). The pillar structure was considered very problematic as the different pillars were comprised of different rules concerning institutions, decision-making instruments and procedures, decision-making powers, judiciary competences and the protection of human rights and fundamental freedoms (Dougan, 2007, p. 617). The Lisbon Treaty abolished the pillar system of the EU. It amended the Treaty on the European Union (TEU) and the EC Treaty by renaming the latter the Treaty on the Functioning of the EU (TFEU). Essentially, the provisions of the former first and third pillars are now found in the TFEU, while the 'distinctive' rules relating to the CFSP are found in the TEU. These amendments have major implications for the right to data protection that will be discussed in detail below.

At this point before the analysis moves on to discuss data protection in the post-Lisbon era, one further major development introduced by the Lisbon Treaty should be mentioned. The EU Charter of Fundamental Rights (EUCFR) was given legal force by the Lisbon Treaty and is now incorporated into European constitutional law (Anderson & Murphy, 2012, p. 155). The Charter, which constitutes the EU's own written bill of rights, enjoys now the same legal value as the Treaties. In fact, the Lisbon Treaty recognizes in Article 6 TEU three formal sources for EU human rights law: the first is the EUCFR, the second is the accession of the EU to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), and the third is the protection of fundamental rights as 'general principles of EU law' that have been developed by the European Court of Justice (ECJ) (now: Court of Justice of the EU (CJEU) over the years.

2.2 The Constitutional Framework for the EU Data Protection Regime

The current constitutional legal base for measures concerning data protection within the EU is Article 16 TFEU. The substantive part of this provision stipulates that "[e]veryone has the right to the protection of personal data concerning them" (paragraph 1). Article 16 TFEU, which replaces Article 286 EC, applies both to the former first and third pillars and provides for the use of the ordinary legislative procedure (Peers, 2011, p. 874) when 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

25 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/data-protection-in-eu-law-after-lisbon/123524

Related Content

Pulse Oximetry: An Introduction
Ashoka Reddy Komalla (2018). *Handbook of Research on Information Security in Biomedical Signal Processing (pp. 130-153).*
www.irma-international.org/chapter/pulse-oximetry/203383

Stuxnet-Tool for Zero-Day Attack
Anita Patil, Swapnil Shindeand Soumi Banerjee (2021). *Handbook of Research on Cyber Crime and Information Privacy (pp. 652-675).*
www.irma-international.org/chapter/stuxnet-tool-for-zero-day-attack/261750

Swarm Security: Tackling Threats in the Age of Drone Swarms
Muhammad Tayyab, Majid Mumtaz, Syeda Mariam Muzammal, Noor Zaman Jhanjhiand Fatimah- tuz-Zahra (2024). *Cybersecurity Issues and Challenges in the Drone Industry (pp. 324-342).*
www.irma-international.org/chapter/swarm-security/340082

A Secure Three Factor-Based Authentication Scheme for Telecare Medicine Information Systems With Privacy Preservation
Kakali Chatterjee (2022). *International Journal of Information Security and Privacy (pp. 1-24).*
www.irma-international.org/article/a-secure-three-factor-based-authentication-scheme-for-telecare-medicine-information-systems-with-privacy-preservation/285017

Critical Evaluation of RFID Security Protocols
Azam Zavvariand Ahmed Patel (2012). *International Journal of Information Security and Privacy (pp. 56-74).*
www.irma-international.org/article/critical-evaluation-rfid-security-protocols/72724