Chapter 18
International Transfers of Personal Data: A UK Law Perspective

Sam De Silva
Taylor Walton LLP, UK

ABSTRACT

Developments in technology and the global nature of business means that personal information about individuals in the UK may often be processed overseas, frequently without the explicit knowledge or consent of those individuals. This raises issues such as the security of such data, who may have access to it and for what purposes and what rights the individual may have to object. The Data Protection Act 1998 provides a standard of protection for personal data, including personal data that is being transferred outside of the UK. This chapter will focus on how a UK data controller (the organisation that controls how and why personal data is processed and is therefore legally responsible for compliance) can fulfill its business and operational requirements in transferring personal data outside the EEA, whilst ensuring legal compliance.

INTRODUCTION

Businesses increasingly operate on an international basis both internally with global group structures and externally with networks of customers and suppliers. This is facilitated by the Internet and information communication technologies which allow the quick and easy transmission of data across national boundaries, and technologies that allow the increasingly complex and cheap collection, storage, use and disclosure of data. The combination of these factors means that personal information about individuals in the UK may often be processed overseas, frequently without the explicit knowledge or consent of those individuals. This raises issues such as the security of such data, who may have access to it and for what purposes and what rights the individual may have to object.

Europe has a long history of data protection and has traditionally been seen as having a higher standard than the rest of the world. European
data protection legislation therefore builds in a standard of protection for personal data that is being transferred outside of the UK. In the UK this protection comes from the Data Protection Act 1998 (the “DPA”), primarily the eighth data protection principle in that Act.

This chapter will address the position in the UK by reference to the DPA, principally the eighth data protection principle. The chapter will then focus on how a UK data controller (the organisation that controls how and why personal data is processed and is therefore legally responsible for compliance) can fulfil its business and operational requirements in transferring personal data outside the EEA, whilst ensuring legal compliance including options such as:

• relying on the findings of adequacy by the European Commission;
• relying on the EU/US Safe Harbor deal;
• using the EU model clauses;
• using Binding Corporate Rules; and
• relying on one of the exemptions in Schedule 4 of the DPA.

This chapter is based on the law as at 1 July 2009.

UK DATA PROTECTION

The law which governs the processing of personal data in the United Kingdom is DPA. The DPA implemented Council Directive 46/1995/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of such Data Within the European Member States (the “Directive”).

The purpose of the Directive and of the DPA is to set the rules for the processing of personal data, the data protection principles, and to give the subject individuals rights in relation to their information and how it is held and used.

In essence the DPA states that the data controller has a duty to comply with the eighth data protection principle (set out in Part 1 of Schedule 1 to the DPA). The eighth data protection principle (see below) is of direct relevance to the international transfer of personal data.

However, it should be noted that other principles and provisions of the DPA are relevant when looking at international transfers of personal data. For example, the first data protection principle requires a data controller to provide information to individuals about the processing of personal data about them. This can include telling people that information about them will go overseas. The seventh data protection principle requires appropriate technical and organisational security measures to be in place to protect data, including ensuring the reliability of staff and having written contracts in place with any data processors (suppliers/providers acting on behalf of a data controller in processing personal information). Compliance with the DPA should be considered as a whole. Although other principles of the DPA are relevant to international transfers, this chapter focuses on the eighth data protection principle.

TRANSFERS INTO THE UK

This chapter addresses transfers of personal data from the UK, but in a global business UK data controllers may also receive personal data from overseas. Some issues to consider in this scenario include:

• Is the UK entity only acting as a data processor on behalf of the overseas entity? If so, the overseas entity may wish to impose contractual obligations on the UK entity but, if the UK entity has no right to use the data for its own purposes, it will not become a UK data controller with compliance obligations.
Related Content

Standards for ICT: A Green Strategy in a Grey Sector
www.igi-global.com/chapter/standards-for-ict/115273?camid=4v1a

ICTs and Border Security Policies in the United States and the European Union
www.igi-global.com/chapter/icts-border-security-policies-united/45396?camid=4v1a

Standardization in Enterprise Inter- and Intraorganizational Integration
www.igi-global.com/article/standardization-enterprise-inter-intraorganizational-integration/2567?camid=4v1a

A Framework to Build Process Theories of Anticipatory Information and Communication Technology (ICT) Standardizing
www.igi-global.com/article/framework-build-process-theories-anticipatory/2588?camid=4v1a