Paul Hastings
StayCurrent
A Client Alert from Paul Hastings
July 2009

European Privacy Directive – Recent Review

BY CHRISTOPHER WALTER AND BEHNAM DAYANIM

In July 2008, the UK Information Commissioner, Richard Thomas, commissioned RAND Europe to prepare an objective, independent report on the strengths and weaknesses of the European Data Protection Directive 95/46/EC. The report was published in May this year; Mr. Thomas hopes it will contribute to the shaping of future data protection laws.

RAND Europe concludes that the Directive will need to change, as society becomes increasingly globalised. While the widely-applauded principles of the Directive will remain useful and relevant, they will need to be supported by a more effective enforcement regime, to cope with the growing challenge of globalisation and international data flows. However, RAND reports that it was also widely recognised that more value can be extracted from better implementation of the current rules, for example by establishing consensus over the interpretation of several key concepts.

The report identifies several strengths in the current regime: its principles have stood the test of time and are flexible in their application; the Directive has helped to harmonise data protection rules across the European Union and provides an international reference model for good practice.

However, certain weaknesses are also highlighted:

- It has unclear objectives and insufficient focus on detriment, risk and practical enforcement.
- It is seen as bureaucratic, burdensome and too prescriptive. The Directive focuses on "how" organisations should do things, rather than on "what" they should be achieving.
- Prescriptive criteria for processing personal data have become a rigid control mechanism. Much effort is devoted to the artificial justification of otherwise unobjectionable processing.
- The Directive's scope is becoming increasingly unclear, for example in on-line and surveillance contexts.
- International transfer rules are unrealistic against a backdrop of high-volume, globalised data flows.

Recommendations

To extract the most out of the current system, RAND proposes that, among other things, Member States should seek agreement on efficient interpretation, implementation and enforcement of the Directive, including encouraging the use of a risk-based approach, ensuring that Binding Corporate

Rules (BCRs) can more easily be used to legitimise data transfers to third countries, improving accountability and helping data processors meet transparency requirements.

Importantly for US-based companies operating in Europe, RAND recommends that the EC should improve scope for finding that the privacy regimes of non-EEA countries provide adequate protection for personal data - and facilitate the use of alternatives to this rule - such as standard contractual clauses and BCRs.

The current adequacy rules are highly restrictive; only countries that follow the Directive are considered to provide adequate legal frameworks for protection. Since the Directive's introduction in 1995, only 5 non-EU countries have been found to have adequate protection regimes: Switzerland, Canada, Argentina, Guernsey, Jersey and the Isle of Man.

The US is only covered through the 'Safe Harbor' Privacy Principles. However, the report notes that companies exporting data to the US may be subject to regulations that exceed the requirement of the Directive, but that are not classified as adequate because they do not constitute a broad, all-encompassing legal framework. Prime examples are the Health Insurance Portability and Accountability Act (HIPAA) and Statement of Auditing Standards No. 70 (part of the Sarbanes Oxley Act), both of which impose certain more stringent requirements on companies than the European regime.

In order to make the European data protection framework viable, given international data flows, RAND proposes an alternative regulatory model based on identifying the desired outcomes in terms of the data privacy expectations of individuals, public/private sector organizations and supervisory bodies and defining global privacy principles:

General Principles:

- Legitimacy – defining when personal data processing is acceptable.
- Purpose restriction – ensuring that personal data is only processed for the purposes for which it was collected, subject to further consent from the data subject.
- Security and confidentiality – specifically by requiring the data controller to take appropriate technical and organisational measures.
- Transparency – that appropriate levels of transparency are provided to data subjects.
- Data subject participation – ensuring that the data subjects can exercise their rights effectively.
- Accountability – that those processing personal data would be held accountable for their actions.

Strong enforcement will be necessary to support these principles. In order to ensure effective and credible enforcement, risk should be the primary criterion employed to determine the amount of fines. Criminal sanctions should be considered for serious incidents or intentional misuse, to act as a deterrent and punishment. Alternative Dispute Resolution may also be considered, to permit easy and quick access to restitution or compensation in low level cases of misuse.

Other European Privacy News

- On May 1 2009, the Information Commissioner's Office (ICO) authorised the intra-company transfer of personal information within the Accenture and Atmel groups. In each case, the ICO

granted authorisation for the data transfers based on the strict rules and procedures put in place by the BCRs, which provide adequate levels of protection for individuals' personal data across borders. This is the first set of BCRs to be approved by a European data protection agency relying on the new mutual recognition procedure that permits a lead EU member agency to bind other European agencies to its decision. Previously, BCRs had to be submitted to and approved separately by the data protection agencies in all relevant countries.

- On April 27, 2009, the Article 29 Working Party issued a new working document (WP 155 rev. 04) on frequently asked questions (FAQs) relating to BCRs. Two new FAQs were adopted: (1) FAQ 10 deals with the relationship between EEA data protection laws and BCRs and (2) FAQ 11 relates to the reversal of the burden of proof in the context of BCRs. The working Party reiterated that although BCRs may offer an adequate level of protection to personal data being transferred across borders they do not exempt multinationals from complying with national data protection laws and taking local compliance steps.

- On April 14, 2009, the EC issued an infringement notice against the UK for alleged breaches of EU data protection laws. The proceedings were prompted by complaints from internet users about the use of behavioral advertising technology by an internet advertising company, Phorm Inc. Phorm's tracker technology enables internet service providers to analyze users' online behaviour in order to build up user profiles and deliver advertising. The EC proposes a range of amendments to UK legislation, including prohibiting unlawful interception and surveillance techniques, without first seeking the users' prior consent ("opt-in" principles).

- *The Personal Data Guardianship Code* was published jointly by the British Computer Society and the Information Security Awareness Forum in response to the number of high profile data breaches in recent years. The new Code is intended to help organisations understand their responsibilities. It aims to promote best practice and provide 'common sense' guidance for data controllers; it also contains useful information for the data subject. Louise Bennett, Chair of the BCS Security Forum, said of the Code: "This is the equivalent of the Highway Code for motorists – it will help all those involved in the management of personal data understand their role and enable them to carry out their jobs better." However, critics assert that the guidance on consent is muddled and inconsistent.

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

London

Christopher K. Walter
44-20-3023-5129
christopherwalter@paulhastings.com

New York

Erika C. Collins
212-318-6789
erikacollins@paulhastings.com

Marjorie R. Culver
212-318-6650
marjorieculver@paulhastings.com

Washington, D.C.

Behnam Dayanim
202-551-1737
bdayanim@paulhastings.com