MORRISON | FOERSTER

Legal Updates & News

Bulletins

Privacy and Data Security: What's in the European Pipeline?

April 2009
by Amina Adam

Privacy and Data Security Update, April 1, 2009

Related Practices:

- Privacy and Data Security

In 2008 we saw an unprecedented level of change in privacy law and practice in the EU. High profile data security breaches ensured that privacy issues remained a priority for both the government and private organisations. Many reforms were proposed to, for example, the Directive on Data Protection 95/46/ECand the e-Privacy Directive 2002/58. We also saw an increase in legislation with the adoption of the UK's National Staff Dismissal Register and the EU's Prum Treaty and the release of the UK's Communications Data Bill. Given the current economic downturn, privacy issues and reforms may remain in a state of flux. We look ahead at what we predict will remain key EU privacy issues in 2009.

International Data Transfer will remain a priority in 2009, given that many organisations transfer data outside of the EU. Organisations that transfer personal data outside of the EU must ensure they comply with the adequacy requirement most commonly by transferring data to an entity that has subscribed to the Safe Harbour Scheme (if the entity is established in the U.S.), or using model contracts or Binding Corporate Rules ("BCRs"). BCRs are an internal corporate data protection adequacy standard that allows for the transfer of data within a group of companies. A company cannot use BCRs to transfer personal data to another company outside of the group, such as in an outsourcing arrangement. In such circumstances, one of the other adequacy mechanisms should be used as appropriate. BCRs must be approved by the various EU Data Protection Authorities ('DPAs'). Many see this as a crunch year for BCRs. Early indications are that companies who have used BCRs are finding the approval process for recognition of BCRs difficult, with regulators becoming increasingly more conservative. It is also a long and costly process. However, thirteen[1] EU DPAs have now joined the mutual recognition procedure, where the DPAs agree to accept the lead authority's approval as the basis for their concurrent approval for recognition. This should make the process easier and less costly and it will be interesting to see if this will result in a greater use of BCRs by multi-national organisations.

Following high profile security breaches in 2008, we expect to see a continued focus on data security breaches. In the UK there is the Coroners and Justice Bill (the 'Bill'), which adopts many of the reforms recommended in the Data Sharing Review report by Richard Thomas and Dr Walport. The Bill was published on 14 January 2009 and includes provisions for increased powers for the Information Commissioner to fine companies for serious data security breaches and to issue assessment and inspections notices. The Bill also gives the Information Commissioner broader inspection rights to carry out unannounced inspections of public sector organisations and makes it a criminal offence to deliberately or recklessly make false statements in response to the new powers to require information. Ministers are now calling for the Information Commissioners' inspection power to extend to private sector organisations.

The Bill also contains provisions which permit a designated authority (e.g. Ministers of government departments, the Treasury and the Secretary of State) to make an information sharing order allowing a person to share information which includes personal data. Whilst an individual affected by the order can make representations, it falls short of obtaining individual consent and therefore this has led to concerns of inadequate protection given the level of information sharing. There will also be a duty on the Information Commissioner to publish a statutory data-sharing Code of Practice and to keep the Code under review.

Other EU countries such as Germany, Ireland, Netherlands and Spain have also proposed reforms to their local data protection legislation. In particular, there are reforms to breach notification and security requirements. Draft legislation in Germany proposes a U.S. style breach notification requirement, increased penalties, voluntary data protection audits by certified organisations and safeguards around the termination of Data Protection Officers. If the draft legislation is approved by the German parliament it is proposed to take effect in July 2009. In Ireland, the Irish Minister for Justice, Equality and Law Reform has set up a reform group that will discuss the introduction of mandatory data breach notification in Ireland. The Reform group was expected to start their work in November 2008 and therefore we expect to see discussions in 2009 on whether the law needs to be changed to deal with data security breaches. In Netherlands, the Chairman of the Dutch Data Protection Authority and the Dutch Public Prosecutor stated in the press that banks and credit card companies should be compelled by law to report the theft of personal data to their clients. Currently they are not under an obligation to do so. In Spain, the Spanish data protection authority has issued a new guide to help companies comply with new data security regulations. The guide applies to both the private and public sector and is aimed at data controllers and data processors. The guidelines clarify which level of security data controllers and processors must apply to specific cases. The guidelines also include a checklist of the issues to be audited, a list of frequently asked questions and a draft Security Document.

Reforms to the EU Directive on Data Protection 95/46/EC will continue to be debated in 2009 and will be discussed at the European Conference of Data Commissioners and by the European Data Protection Supervisor ('EDPS'). Proposed reforms include the definition of controller and processor and questions relating to applicable law.

A Working Party 29 subgroup is currently addressing the implications of U.S. e-discovery actions in the EU, pursuant to which personal data of EU citizens are requested to be transferred to the U.S. for use in litigations and investigations. A working document on pre-trial discovery for cross-border litigation was adopted on 11 February 2009. We expect to see in 2009 further discussions by the European Commission on the issues raised by the Article 29 Working Party.

There is ongoing debate in the EU on the ePrivacy Directive 2002/58 which relates to telecommunications reforms, including setting up a data breach notification system to inform individuals when their personal information has been compromised, which entities should notify them of breaches, what the trigger for notification is and who should be the recipient of the notification. At present the European Council of Ministers and the European Commission do not support expanding the scope of an EU security breach law beyond telecommunications companies. In contrast, the European Parliament, the EDPS and the Article 29 Working Party have expressed support for a security breach notification requirement that would cover all companies providing online services. The issue will now be debated at the European Parliament in an attempt to find a compromise that can be passed into EU law.

In 2009 the EU and the U.S. will start negotiations to create a binding international agreement on data-sharing between law enforcement agencies for the purposes of combating terrorism and international crime. The agreement will be based on the twelve privacy principles drawn up by the U.S. and EU High Level Contact Group to ensure minimum standards for data processing and data-sharing between the EU and the U.S.

There will also be privacy challenges in areas of technological development, for example regarding targeted online advertising and social networking sites. We may also see Privacy Impact Assessments used more widely in the UK in 2009.

In the current economic climate we would advise organisations to continue to prioritise privacy issues as compliance will only become increasingly scrutinised by regulatory bodies and penalties for non-compliance increase in amount and frequency. Data transfers will also remain a key issue in any sale of a business or in any outsourcing arrangement.

Footnotes

[1] France, Germany, Ireland, Italy, the United Kingdom, the Netherlands, Spain, Latvia, Luxembourg, Norway, Iceland, Liechtenstein and Cyprus.
