The diversity of harmonisation

With the ten new EU countries' different historical and legal cultures, the data protection harmonisation process reflects their diversity of approach as much as their common objectives, says **Stewart Dresner**.

When you try to compare the data protection laws of the 10 new EU accession countries, a lawyer's technical analysis is necessary but not sufficient. It gets you only so far. The commonalties with the EU Data Protection Directive provide a framework for analysis but lack the national contexts. Without this dimension, understanding is incomplete and distorted.

Take, for example, the comments made by the Council of Europe's (CoE) Czech Ambassador at a conference in Prague last month. Vlasta Stepova succinctly explained that, "Under the former [communist] regime, the government knew everything about the people. Therefore, protecting personal data is a new concept. We have to learn again what it is to be a human being."

Dr Karel Neuwirt, President of the Czech Republic's Office for Personal Data Protection and Chairman of the CoE conference, leads a team energetically pursuing this learning process. His helpline service, handling enquiries from individuals and organisations, is helping all parties to develop a mutual understanding of how data protection law should be interpreted. Publications from his office are also helping to spread the word on issues such as medical testing and the deduction of trade union dues by employers. Dr Neuwirt is also proactive in engaging with different sectoral groups, seeking consensus where possible.

Poland, on the other hand, emphasises rigorous enforcement. The Inspector General, Dr Ewa Kulesza, last year carried out 184 inspections and referred 74 cases for criminal prosecution. There are tough sanctions for breaching Poland's Data Protection Act, including possible prison sentences of up to three years for illegally processing sensitive personal data.

Hungary, by contrast, until recently had no powers to conduct such inspections and placed less emphasis on criminal sanctions. The resulting emphasis on dialogue has encouraged Dr Attila Peterfalvi, the Parliamentary Commissioner for Data Protection and Freedom of Information to use his independent and prominent status in Hungarian society to good effect.

This position is a result of Hungary's data protection law winning a rare majority of more than two thirds of the legislature. Dr Peterfalvi meets legislative committees and, when necessary, voices criticism of the law he is charged with supervising. One example is the law's data export rules, which state that transfers to countries that the European Commission has not declared adequate are illegal. The Hungarian Commissioner wants to avoid this onerous burden placed on businesses and is seeking a change in the law that will permit data transfers while ensuring that EU data protection standards are met.

Data Transfers - The Hungarian Commissioner wants to avoid this onerous burden placed on businesses and is seeking a change in the law that will permit data transfers while ensuring that EU data protection standards are met.

It was clear, at November's European Privacy Officer's Network (EPON) meeting in Prague with the data protection authorities from these three countries that each authority has its own priorities and attitudes. Their laws do not always permit them to offer ready-made legal solutions to the issues companies face. But despite their national differences, they generally show a willingness to work with companies and to recognise when they are making genuine efforts to respect and comply with their laws. The authorities are also actively engaging in new initiatives such as the binding corporate rules scheme for international data transfers (see p.7).

In some of the accession countries, such as Poland, the law has met with public indifference. In others, for example Cyprus, Goulla Frangou, Commissioner for Personal Data Protection, reports that interest is easily sparked by issues that capture the public's attention. Where the public is engaged, they want action against organisations that have broken the law. The public are not satisfied by mere changes to management practice. They expect that fines, if imposed, should be used to compensate those who have suffered.

The EU directive remains the standard. But, just as there are many differences between the way national data protection laws are enforced in Western Europe, substantial differences remain in the differing legal cultures represented by the 10 new EU accession countries.

Meanwhile, those countries adjacent to the 25 EU member states, are paying close attention. At the CoE conference in October, there were representatives from many such countries including Albania, Croatia, Romania, the Russian Federation, Macedonia and the Ukraine. While some, such as Croatia, have established a Personal Data Protection Agency, others combine this function with other ombudsman responsibilities, as in the case of Romania. In Russia and the Ukraine, the priority is data protection in the sense of data security and this work is handled by the Security Services.

AUTHOR:

Stewart Dresner, Chief Executive, Privacy Laws & Business

CONTACT:

stewart@priavcylaws.com

Safe Harbor, continued from p.3

enforcement action. The FTC has powers to pursue companies which make false or misleading statements in their privacy policies, but it is doubtful whether it would have jurisdiction over those that fail to actually publish the required statements. In those cases, says Professor Reidenberg, "it would be very hard for any kind of enforcement action to proceed in the United States."

Iron glove, velvet hand

The European Commission is now calling for US authorities to implement a number of actions, ranging from minor technical changes to the Safe Harbor registration system, through to taking a more proactive stance on enforcement. But considering that little has changed since the last Safe Harbor status report in 2002, the question is whether the Commission has the will to stand its ground and prevent the programme from degenerating into nothing more than a paper tiger. And if the US authorities fail to comply, could the Commission ultimately threaten to wind up what has effectively become a paper tiger. "I don't think in the near term Safe Harbor will be scrapped," says Professor Reidenberg, suggesting the EU has more pressing concerns on the privacy front – most notably US demands for access to European air travelers' flight details (Passenger Name Record (PNR) data). "I think Europe would be more likely to push PNR and not confuse that issue with the private sector conflicts," he says.

Dr Bygrave argues that although the Commission needs to push forward changes, a heavy handed strategy could prove counterproductive. "While there is much that can be criticised with respect to Safe Harbor, it would be premature to scrap it now," he says. "US companies and authorities need to be given more time to incorporate European data protection principles and ideals into their respective organisational cultures."

Double standards?

US authorities may need to be more proactive on enforcement, but the same is true of the European regulators who also have a role to play in making the programme a success. By showing greater interest in Safe Harbor and making US companies aware that their practices are under scrutiny, says Dr Bygrave, EU data protection authorities stand a greater chance of persuading them to comply.

The Commission's report has revealed flaws in Safe Harbor, but the consensus of opinion is that it is perhaps too early to think about wrapping up the programme. If it is to become a viable tool for international data transfers, the authorities on both sides of the Atlantic will need to become far more active.

AUTHOR:

Alan Pedersen, Editor, *PL&B International*

CONTACT:

alan@privacylaws.com

Safe Harbor status report - Results and recommendations

Published in October and funded by the European Commission, the *Safe Harbor Decision Implementation Study* is an independent report carried out by legal academics in Belgium, Norway and the United States. Below is a summary of the report's key findings and recommendations. The full text can be found on the Commission's website: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

Compliance with Safe Harbor Principles

Organisations signing up to the Safe Harbor programme are required to comply with seven privacy principles (notice, choice, onward transfers, access, security, data integrity, and enforcement). In order for Safe Harbor registration to be valid, organisation's must acknowledge compliance with these principles through a publicly available privacy policy.

Report findings: The Safe Harbor report found that a "relevant" number of companies were failing to address Safe Harbor principles in their public privacy policies. Some organisations were either ambiguous and vague over their use of personal data, or failed to provide any information at all. A number of organisations did not offer individuals the right to opt-out from external data sharing, or allow full access to their personal records.

Recommendations: The report has called for the US Department of Commerce (DoC) to publish guidelines for organisations on how to correctly draft Safe Harbor privacy policies. Additional suggestions include providing greater clarification on key privacy concepts (such as 'personal data' and 'anonymous data') to make privacy policies more comprehensible.

Self-certification procedure

The Safe Harbor establishes a self-certification process in which companies make a declaration to the DoC that they are in compliance with the Safe Harbor principles. The DoC is responsible for handling the registration process which can be carried out via its Safe Harbor website (www.export.gov/safeharbor/index.html).

Report findings: While the DoC has generally met its obligations, the report has raised some technical issues on the DoC website. For example, organisations exporting human resources data to the US must agree to 'comply' with decisions made by European data protection regulators - yet the DoC's online certification form mentions only 'cooperation' with the regulators. The report argues that this is not enough to sufficiently bind participating organisations.

Recommendations: Changes to the DoC's Safe Harbor website are recommended in order to tighten up the self-certification process and make the site more user-friendly. The European Commission has also called on the DoC to be more proactive in scrutinising the documentation submitted by participating companies.

Enforcement mechanisms

The main Safe Harbor enforcement body is the US Federal Trade Commission (FTC). Because participating organisations signify compliance through their privacy policies, failure to abide to their commitments can trigger enforcement action under the unfair or deceptive practices provision of the Federal Trade Commission Act.

Report findings: A lack of adequate enforcement means that some organisations are operating below European privacy standards. Concerns have also been raised over whether the FTC - which is limited to regulating deceptive practices affecting commerce - has sufficient jurisdiction over human resources (HR) data.

Recommendations: The FTC has been encouraged to be more proactive in monitoring and investigating compliance. The report also calls for clarification over the FTC's jurisdiction on HR data.