Editorial

Bridget Treacy discusses moving from theory to practice — delivering real data protection, for Volume 10, Issue 8, of Privacy & Data Protection

We readily acknowledge the central role of data in our information-based economy, and accept the need to safeguard data assets. Yet, despite the growing roll call of serious data breaches and the best of intentions, many organisations still fail to embed data protection into the core of their information governance strategy. In proposing the formal inclusion of an 'accountability' principle in the revised data protection framework (see Working Paper 173), the Article 29 Working Party strikes at the heart of the issue: how to deliver real data protection.

The concept of accountability is not new. It appears explicitly in the Organisation for Economic Cooperation and Development's privacy guidelines adopted in 1980, in the Canadian Fair Information Principles, in the Asia-Pacific Economic Cooperation privacy framework and its cross border privacy rules and, most recently, in the Madrid International Standards. The concept of Binding Corporate Rules is an example of how the accountability principle might work in practice in an EU data protection context. But what does accountability mean in practical terms, for organisations of all sizes, and how might it help make data protection 'real'?

The Working Party describes the concept of accountability as the means by which an organisation demonstrates how it exercises responsibility for data protection, and how this can be verified. Crucially, accountability does not impose additional data protection principles or responsibilities on organisations, nor does it absolve them from compliance with existing principles. Rather, the concept makes explicit the need for organisations to (i) take appropriate measures to implement data protection principles; and (ii) provide evidence that such measures have been taken.

In practical terms, this means that organisations must implement internal procedures to give effect to existing data protection principles. Organisations should have data protection policies, privacy notices, adequate security measures, training programmes, and procedures for ensuring that individuals may exercise their rights. In addition, the existence and effectiveness of these measures must be demonstrated or verified. These are familiar concepts, but ones that are often not realised in many organisations.

In other words, the concept of 'accountability' envisages that organisations implement and demonstrate adherence to a comprehensive data protection compliance programme. The Working Party proposes practical tools to assist in creating such a programme, and compliance should be verified by third party certification agents. This latter step is significant. Data protection authorities often do not have the power to verify compliance with local data protection requirements. Even those that do have the power to conduct audits and inspections do not have the resources to do more than verify compliance at a handful of organisations.

A more effective use of the regulators' resources would be to require organisations to take appropriate steps to verify compliance and to be able to provide evidence of compliance on request.

For organisations, the explicit adoption of an accountability principle would provide flexibility. Organisations would be able to tailor their programmes to reflect the risks associated with their specific data processing activities.

The adoption of the accountability principle envisages data controllers retaining flexibility in terms of how they discharge their obligations under applicable local data protection law, but requires them to be able to demonstrate how they achieve compliance. It would also encourage (but not require) organisations to adopt 'bespoke' data protection programmes which tailor their business models to data protection principles, but do not impose prescriptive and bureaucratic requirements of little practical value. Such an approach would of course target enforcement against those who are unable to demonstrate any attempt at compliance.

If organisations adopted the accountability principle, it would simplify the data protection regulator's task and, in some respects, is a natural extension of the approach to regulation adopted in the UK. As such, it may also generate greater trust in organisations' data processing arrangements, and reduce the burden on those data controllers who take data protection seriously and can demonstrate that they are accountable.

It might also be the case that individual data protection authorities would move away from mandatory prior notification of data processing activities provided that they are satisfied with the certification standards applied by third party agents. Further, there would be a greater focus on the role of a controller, with the mandatory appointment of data protection officers a distinct likelihood.

The Working Party's approach that should be embraced by individuals, organisations and regulators alike. Hopefully, the Commission will agree that the adoption of the concept of accountability will help to ensure that "data protection becomes part of the shared values and practices of an organisation, and that responsibilities for it are expressly assigned."

Bridget Treacy
Hunton & Williams
btreacy@hunton.com