

Alert 10-187



Article 29 Working Party Opinion 3/2010 on the Principle of Accountability: 'Made to Measure' Data Privacy Compliance for the Proactive?

Introduction

On July 13, 2010, the influential Article 29 Working Party (Working Party), consisting of all the European Union's national data privacy regulators, adopted Opinion 3/2010 on the principle of accountability (Opinion).

This is an important contribution to the European Commission's review of the European Data Protection Directive 95/46/EC (Data Protection Directive), a draft of which had been expected later this year, but is now expected some time in late 2011.

In essence, the Opinion builds on good practice in the area of global regulatory compliance, advocating the introduction of a "principle of accountability" in the revised Data Protection Directive that "would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the [Data Protection] Directive and demonstrate this on request." The Working Party objective is to "encourage data protection in practice" by requiring data controllers to take a strategic, risk-based approach when determining effective and appropriate measures based on the nature of the personal information being processed and the risks represented by such processing.

Accountability - background

Accountability is an established concept in global compliance terms, and the Opinion clearly signals that it is a concept whose time has come given the "*data deluge*" effect facing controllers, regulators and the general public alike, from:

- The exponential growth in the amount of personal data processed and transferred
- Increased technological developments and user interaction with such technologies; and
- Increased risks of data breaches as more data is available and travels across the globe

The accountability principle first appeared in international guidelines on data protection published by the Organisation for Economic Cooperation and Development (OECD) nearly 30 years ago, and it also features in the Asia-Pacific Economic Cooperation Privacy Framework as well as Canada's Federal Privacy law and numerous legal and academic texts and treatises on the subject. Accountability was most recently included in the Madrid Resolution of 2009 adopted by the International Conference of Data Protection and Privacy Commissioners, consisting of 80 data protection authorities from 42 countries around the world, including members of the Working Party.

Accountability - what does it mean in practical terms?

While the Working Party recognises that defining "accountability" is not straightforward, its aim is to encourage the development and adoption of:

- Practical and concrete measures defined at the level of the controller
- Controllers' responsibility to demonstrate the effectiveness of such measures

- Transparency to both individuals and the general public

by controllers taking appropriate and effective measures to implement data protection principles and demonstrating upon request that such measures have been taken.

When implementing the kind of measures envisaged – for example, a policy and process for dealing with subject access requests – the Opinion makes it clear that the "assignment of responsibilities" and the "training of staff involved in the processing operations" are indispensable to ensuring that the responsibilities at different levels of the organisation are fulfilled.

When it comes to demonstrating the effectiveness of such measures, the Opinion refers to monitoring, internal and external audits, and other control and oversight mechanisms familiar to organisations, based on established compliance programs in other regulatory fields; for example, SOX or FCPA compliance.

The Opinion sets out a non-exhaustive list of "*common accountability measures*" for consideration, which begins with establishing internal procedures and developing effective measures prior to any new processing of personal data, and suggests appointment of a responsible data protection officer with sufficient resources allocated for privacy management, training and awareness.

Accountability ensures that data protection is built into all strategic decisions of an organisation and assesses the risk and seeks the involvement of all levels of an organisation by advocating that controllers conduct privacy impact assessments and other "proactive measures", such as:

- Data loss/breach detection/prevention policies and procedures
- Using "Privacy by Design" to develop and implement new technologies
- Binding policies and procedures that measure compliance
- Response plans that draw on lessons learned, mitigate harm and avoid future breaches

The Working Party envisages preparing general guidance setting out "a baseline of necessary elements for a standard data controller" and for large organisations "a model data compliance program."

Looking (and Planning) Ahead

It is going to be several years before any revised Data Protection Directive is agreed and in force throughout Europe. In the meantime, organisations are encouraged to follow the lead of an increasing number of data controllers who are taking responsibility for their data privacy obligations through the adoption of robust data privacy compliance programs. In so doing, they are holding themselves accountable to their stakeholders, including data protection authorities and data subjects, for that commitment to good practice.

The Working Party suggests that not only are such organisations more likely to be in compliance with the law, but, in the event of a data protection violation, data protection authorities also "*could give weight to the implementation (or lack of it) of measures and their verification in considering sanctions.*"

How might we help?

The Opinion is an important output of the Working Party and provides a clear indication of how the European data protection authorities view the real-world challenges facing data controllers.

Reed Smith's Data Security, Privacy & Management Team has the level of experience and "hands-on" knowledge and practical experience required to support you in designing, developing and implementing data privacy compliance programs, including advising clients on the full range of effective measures identified.

→ [Cynthia O'Donoghue](#) Partner
London
+44 (0)20 3116 3494

→ [Nick Tyler](#)
Associate
London
+44 (0)20 3116 3695

About Reed Smith

Reed Smith is one of the 15 largest law firms in the world, with nearly 1,600 lawyers in 22 offices throughout Europe, the Middle East, Asia and the United States.

Founded in 1877, the firm represents leading international businesses from FTSE 100 corporations to mid-market and emerging enterprises. Its lawyers provide litigation and other dispute resolution services in multi-jurisdictional and high-stake matters, deliver regulatory counsel, and execute the full range of strategic domestic and cross-border transactions. Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, advertising, technology and media, shipping, energy trade and commodities, real estate, manufacturing, and education. For more information, visit reedsmith.com.

Europe: [London](#), [Paris](#), [Munich](#), [Greece](#)

Middle East: [Abu Dhabi](#), [Dubai](#)

Asia: [Hong Kong](#), [Beijing](#)

United States: [New York](#), [Chicago](#), [Washington](#), [Los Angeles](#), [San Francisco](#), [Philadelphia](#), [Pittsburgh](#), [Oakland](#), [Princeton](#), [Northern Virginia](#), [Wilmington](#), [Silicon Valley](#), [Century City](#), [Richmond](#)

The information contained in this Client Alert is intended to be a general guide only and not to be comprehensive, nor to provide legal advice. You should not rely on the information contained in this Alert as if it were legal or other professional advice.

Reed Smith LLP is a limited liability partnership registered in England and Wales with registered number OC303620 and its registered office at The Broadgate Tower, 20 Primrose Street, London EC2A 2RS. Reed Smith LLP is regulated by the Solicitors Regulation Authority. Any reference to the term 'partner' in connection to Reed Smith LLP is a reference to a member of it or an employee of equivalent status.

This Client Alert was compiled up to and including August 2010.

The business carried on from offices in the United States and Germany is carried on by Reed Smith LLP of Delaware, USA; from the other offices is carried on by Reed Smith LLP of England; but in Hong Kong, the business is carried on by Richards Butler in association with Reed Smith LLP (of Delaware, USA), and in Beijing, by Reed Smith Richards Butler LLP. A list of all Partners and employed attorneys as well as their court admissions can be inspected at the firm's website.