

**Centre for Information Policy Leadership
at Hunton & Williams LLP**

**A New Approach to International
Transfers**

**In Response to the European
Commission's Communication on
"A comprehensive approach to
personal data protection"**

January 2011

Executive Summary

Reforming the regime for international transfers is by far the most pressing priority for reform of the EU Data Protection Directive. There is a paradox that substantial resources are expended by some organisations trying to “get it right” (if only in legal paperwork) whilst there is unmeasured non-compliance by other organisations which ignore the requirements. This discredits the EU legislation and does little to secure genuine data protection when personal data leaves Europe.

We believe that a new framework for international data transfers, built on the experience with BCRs and explicitly grounded on the Accountability principle, could be achieved with “**Binding Global Codes**” (BGCs). This approach addresses the scale of the challenge with millions of transfers occurring daily, but without the current (but inevitable) delays and bureaucracy associated with BCRs.

The BGC proposal allows an organisation to develop and implement its own bespoke Code with a set of binding rules for demonstrating and ensuring compliance with the Data Protection Principles and their practical implementation on a worldwide basis. The Code must be publicised and the organisation must be held accountable for fulfilling its terms. This means that DPAs would be empowered to investigate and impose meaningful sanctions in any case where either the Code itself does not impose sufficiently rigorous standards or the organisation has failed to meet the requirements of its own Code.

This paper concludes with a first draft of legislation to illustrate the approach that we have in mind for inclusion within a new Directive or Regulation.

1. Introduction

1.1 The Centre for Information Policy Leadership, associated with Hunton & Williams, encourages responsible information governance in today's digital society. Through collaboration with industry leaders, civil society and consumer organizations and government representatives, it explores innovative and pragmatic approaches to global policy issues, seeking to build privacy and data protection in practice while balancing economic and societal needs and interests. More details about the Centre can be found at www.informationpolicycentre.com.

1.2 This Paper is complementary to the Centre's main Commentary responding to the European Commission's Communication on “A comprehensive approach to personal data protection”. The purpose of this separate and self-contained Paper is to set out in more detail our proposals for a new approach to international data transfers. We are proposing a new legislative framework for transfers undertaken in accordance with the

Accountability principle, which will achieve good standards of data protection in accordance with the EU Data Protection Principles on a world-wide basis. We would be delighted to discuss our proposals at a further level of detail through meetings or correspondence with the Commission.

1.3 The Centre welcomes the Commission's recognition that the challenges of technology and globalisation are now driving the need for reform with unprecedented urgency. We see the issue of international transfers as by far the most pressing priority for reform. Articles 25 and 26 of the existing Directive have been simultaneously its most controversial and most burdensome provisions. It is also arguable that they have been the least effective if full account is taken of current volumes of international transfers. The wish to protect EU citizens on a worldwide basis when their personal data is transferred is understandable and not in doubt.

1.4 We therefore wholeheartedly welcome the commitment to "improve and streamline" arrangements for international transfers. But we are disappointed that the Commission's thinking appears to be still incomplete and that concrete suggestions have not yet been put forward. Moreover, we are sceptical about the value or practicality of "clarifying" the Adequacy procedure and there are well-rehearsed problems or limitations with standard contract terms and the Safe Harbor arrangement. At the moment is the paradox that substantial resources are expended by some organisations trying to "get it right" (if only in legal paperwork) whilst there is unmeasured non-compliance by other organisations which ignore the requirements. This discredits the EU legislation and does little to secure genuine data protection when personal data leaves Europe.

2. Binding Corporate Rules – Successes and Limitations.

2.1 The optimum international framework for international data transfers needs to recognise that good data protection cannot arise from laws, rules, policies and procedures alone. It is now also a matter of corporate and information governance, needing:

- top leadership and managerial commitment;
- IT enhancements and safeguards;
- employee awareness, training and supervision;
- cultural reinforcement; and
- incentive and deterrent pressures driven largely by considerations of organisational reputation.

2.2 The Binding Corporate Rules (BCR) approach – originally documented by the Article 29 Working Party in 2003 and developed in further Opinions since then - has been a welcome attempt in principle to address these challenges. It is widely seen as a brave attempt to improve the protection of fundamental rights in the international context. European DPAs deserve recognition and credit for developing and exploring BCRs as a way to address these challenges.

2.3 The BCR approach has *in principle* been attractive to businesses and regulators and has generated positive responses. Businesses especially value the scope for tailoring their own BCR within a template of minimum requirements to address their own circumstances. This approach recognises that good practice for data protection - applying general principles to particular circumstances – is inevitably context-specific. This approach is a good example of modern co-regulation. It is also an excellent example of the Accountability Principle which the Centre has supported through the Galway and Paris projects. The two main Discussion Documents are “*The Essential Elements of Accountability*”¹ and “*Demonstrating and Measuring Accountability*”².

2.4 However the **problems** associated with BCRs – principally delay and expense – are now **very serious**. Although the pace has quickened in the last two years, very few BCRs have actually been delivered. (It is thought that fewer than 20 BCRs have so far been approved or are near to approval.) Delays occur both in negotiations with the lead DPA and in securing clearance from the other 26 DPAs across the EU, even where the Mutual Recognition agreement applies. The causes of delay arise from novelty, unfamiliarity, complexity (legal, cultural, corporate) and the wide differences from one type of multinational organisation to another.

2.5 Above all, however, the problem is lack of resources within DPAs. BCRs are concentrated within a few lead authorities, and those authorities are limited in their ability to expand resources.

2.6 Moreover, the relentless expansion of the digital society means that the authorities must place greater priority on effective enforcement against (or guidance for) those organizations which deliberately, ignorantly or cavalierly make little or no effort to protect personal data. It will be increasingly untenable for DPAs to devote growing attention to the **lower** priority of BCR negotiations (where broadly well-intentioned businesses are trying to get it right).

2.7 A 2003 Yale study conservatively estimated that there are some 63,000 multinational corporations, with 821,000 subsidiaries. They directly employ 90 million people and produce 25 per cent of the world's gross product. It can be asserted with confidence that that every single multinational corporation now transfers personal data internationally. Beyond that, there are countless SMEs and other organisations which are not “multinationals”, but which are nevertheless involved daily in international transfers of personal data, often of a highly sensitive nature. In short, it is inconceivable that the BCR approach – without improvement - could meet the potential underlying demand.

2.8 In summary, the BCR approach is therefore now facing:

the risks of failure – businesses will give up or not apply; and / or

¹ http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

² http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

the risks of success – even if more BCRs are approved, DPAs will become totally swamped and delays will get much worse and paralyse the entire system.

This situation will seriously **damage the credibility** of BCRs, of European DPAs and of all attempts to regulate international data transfers.

A new approach – modernisation building on conceptual success with BCRs – is now needed with some urgency. New features (substantive and process) must aim at (1) improving the attractions to businesses (who will wish to minimise the burden) and (2) improving the value to regulators (who will wish to increase their effectiveness in securing maximum levels of compliance and good practice). A new approach must realistically migrate from the test-bed of very low volumes to mass-production.

3. Accountability in Practice

3.1 The Galway and Paris Projects have put Accountability firmly on the agenda, both generally and within the context of reform of EU data protection law.

3.2 The essential elements of Accountability can be summarised as:

- organisational commitment to **bespoke** internal policies which elaborate the general Principles
- mechanisms to develop and put policies into effect, including procedures, technologies, training and education
- systems for ongoing internal oversight, assurance reviews and external verification
- focus on risks and outcomes
- transparency
- readiness to **demonstrate** the chosen approach to compliance.

3.3 Accountability reinforces – but does not replace – legally binding ways for ensuring respect for the fundamental right to data protection. But its flexibility and encouragement for tailor-made policies and procedures to fulfil the Data Protection Principles also reflect that responsible companies want or need to process personal data properly. A statutory requirement for putting the essential elements of accountability into effect, as recommended by the Article 29 Working Party, would expand the number of responsible organizations and facilitate more effective enforcement.

*“..it would be appropriate to introduce in the comprehensive framework an accountability principle...[This] would require data controllers to have the necessary internal mechanisms in place to **demonstrate compliance** to external stakeholders, including national DPAs.....”*

“The new provision could be included....even in the case the data have been

transferred to other controllers outside the EU.”

*Article 29 WP / WP on Police & Justice
The Future of Privacy, Dec 2009*

“Data protection must move from theory to practice. Legal requirements must be translated into real data protection measures”

“One size does not fit all”

“[Accountability offers ways to] implement appropriate and effective measures to put into effect the Directive’s Data Protection Principles and obligations”

*Article 29 WP Opinion on Accountability
July 2010*

3.4 Although this is not explicit, accountability has in fact always been the foundation of the BCR approach. In effect, adherence to a set of Binding Corporate Rules signifies that a business is prepared to demonstrate its commitment to compliance and good practice and can be held accountable (by regulators and stakeholders) for fulfilment of that commitment.

*The [BCR] rules are expected to set up a system which guarantees awareness and implementation of the rules both inside and outside the European Union. The issuing by the headquarters of internal privacy policies must be regarded only as a first step in the process of adducing sufficient safeguards within the meaning of Article 26 (2) of the Directive. The applicant corporate group **must also be able to demonstrate** that such a policy is known, understood and effectively applied throughout the group....”*

*Article 29 WP
WP 74, Binding Corporate Rules, 2003*

4. Binding Global Codes

4.1 We are proposing a new approach - **Binding Global Codes (BGCs)** – based on the following propositions:

- The BGC Framework would be built on an explicit foundation of Accountability.
- A multinational organisation which adopts and implements an acceptable Binding Global Code would accept responsibility for its fulfilment and for ensuring delivery of fundamental rights. In return – and for so long as that remains true - it would be treated as satisfying EU and other requirements for international data transfers.

- A Binding Global Code would take the form of a set of binding rules demonstrating compliance with the Data Protection Principles on a worldwide basis and meeting certain other minimum requirements.
- The Code must cover policies, procedures, technology and human/organisational issues – not just legal compliance - with clear governance arrangements and identifiable internal responsibility.
- The governance arrangements should extend to mandatory internal assurance or verification arrangements
- The Code must apply globally to all processing by the organisation of personal data (unless explicitly excluded) and (by contract) to all those with whom the data is shared.
- The code must be formally adopted by the organisation through a defined standard procedure.
- The Code must be publicised and the organisation must be held accountable for fulfilling its terms. Publicity could be mandated through website notices, media announcements, annual reports, filing with regulators and listing bodies etc.
- Organisations would self-certify their own Code without the need for prior DPA approval, which is simply not practicable with the scale of the challenge.
- DPAs would be empowered to investigate and impose meaningful sanctions in any case where either the Code itself does not impose sufficiently rigorous standards in line with the Data Protection Principles or the organisation has failed to meet the requirements of its own Code. This is consistent with the emphasis which we place elsewhere on action against false or misleading privacy statements.
- If self-certification is considered too radical, there are other options for the initial adoption or approval of a Binding Global Code to ensure that the minimum requirements are in fact met. These include certification by an independent Third Party (“Accountability Agent”) appointed by the DPA at the expense of the business or certification by a Third Party approved by the DPA.
- There is a corresponding need for meaningful sanctions – injunctive, punitive and remedial - where an organisation fails to fulfil its own Code. Accountability means facing the consequences of failure, including failure to fulfil publicly-adopted commitments.
- With scope to re-direct resources more effectively, a new priority for regulators – collaborating internationally – must be to enforce compliance in practice. The emphasis would be on holding

organisations to account for the commitments they have assumed by adopting their Code. Effective regulatory interventions must be expected where:

- the content of a Binding Global Code in fact fell below the requirements;
 - inspection or audit reveals non-compliance with commitments given in the Code;
 - complaints or incidents reveal such non-compliance;
 - self-declaration – e.g. where the organisation is required to notify the regulatory or listing authority of specific or systemic non-compliance.
- Individuals would be entitled to pursue claims against an organisation where liability arises because they are denied the rights guaranteed to them under its Code.
 - To the extent that mandatory requirements of local law are inconsistent with the BGC approach, such requirements would need revision, probably at EU level.
 - The BGC approach has the potential to align with equivalent provisions in the APEC Privacy Framework to achieve a genuinely global solution, but perhaps with the robust substance which would flow from European leadership.

4.2 To summarise, a Binding Global Code would be the vehicle for the organisation to handle international flows of personal data in ways which are lawful, which ensure standards of good practice respecting the integrity of the data and which bring internal discipline to the business. Organisations striving to handle personal data well, in compliance with legal requirements and good practice, would have a major incentive for adopting a Code – provided they can avoid the burden and delay of advance negotiation and prior approval.

5. Suggested Legislation

5.1 We will be happy to participate in further discussions to develop the BGC approach further. At this stage, the following text, based otherwise on the provisions of the existing Directive, is a first draft to illustrate the approach that we have in mind:

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, a data controller (or member of its corporate group [as defined]) may transfer personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) on condition that:

- a. the transfer takes place in accordance with a Binding Global Code adopted by that data controller; and
 - b. the data is processed, and continues after transfer to be processed, in accordance with that Code.
2. A “Binding Global Code” means a set of legally binding rules which require contractually or otherwise, that regardless of location:
 - a. the personal data will be processed in accordance with the principles and obligations set out in the Directive; and
 - b. adequate safeguards will be observed with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.
3. “Legally binding” means that:
 - a. the rules are legally enforceable and binding in practice so that the controller is liable, whether to a supervisory authority or to any adversely affected data subject, for any non-compliance with them; and
 - b. the controller is committed to demonstrate to a supervisory authority on request how compliance is and will be achieved.
4. A Binding Global Code shall also contain other measures, including those of a technical or organisational nature, directed at promoting compliance with the principles and obligations set out in the Directive and with good practice in the processing of personal data.

The views expressed in this paper are those of the Centre for Information Policy Leadership. They do not necessarily reflect the views of the Centre’s members or those of Hunton & Williams LLP or its clients.