
# Accountability, Risk Assessment and Binding Corporate Codes.

**DRAFT: March 2013**

## The challenge

Any privacy / data protection law should be effective in terms of ensuring strong protection, but without imposing disproportionate administrative burdens or threatening innovation.

The draft EU Regulation of January 2012 has been criticised on a number of grounds. Some of these are inter-related and are addressed in this proposal. They include:

- too prescriptive (especially much of Articles 22-37), not contextualised and with too much of a "One size fits all" approach;
- insufficient focus on "tick-box" compliance, at the expense of improving information governance in practice;
- mis-application of the Accountability principle, using it to justify new and inflexible burdens;
- not sufficiently outcome-focused;
- arbitrary and inappropriate exemptions (largely based on corporate size);
- too burdensome on DPAs, and impedes prioritisation on the willful, the cavalier and the non–accountable (i.e. *not* "Selective to be Effective");
- mis-alignment between rules for international transfers and "domestic" rules;
- insufficiently risk-based.

Some of these concerns have been recognised. In a December 2012 speech , Viviane Reding said :

> *"I am willing to consider following a more risk-based approach…..Such an approach doesn't just mean "Let data controllers choose what they will do"…. Instead, we want to build an approach that adequately and correctly takes into*

*account risk. The approach also has to be simple….We want to make sure that obligations are not imposed except where they are necessary to protect personal data."*

In the same month, the Presidency Note to the Council of Ministers recorded that

*"Many delegations stated that the risk inherent in data processing operations should be the main criterion for calibrating the applicability of data processing obligations….There appears to be a general consensus that [we] should aim at introducing a strengthened risk-based approach into the draft Regulation……..The risks will need to be balanced against entrepreneurial freedom and the tasks of the public sector…. Obligations [should therefore be] calibrated to the nature of the processing and of the data...and in relation to their impact on individuals' rights and freedoms."*

Concrete proposals to fulfill such new thinking have so far been missing. This proposal therefore outlines a new approach, with suggested legislative text. Its key features include:

- elaboration of a risk-based approach based on specific threats to data subjects;
- an Accountability principle based upon a wide consensus of how this should function in practice;
- the principle (as in the draft Regulation) that all Data Controllers should held accountable for a basic level of compliance…..
- …..but calibrated with more rigorous requirements where there is a significant risk of serious harm;
- a comprehensive privacy programme known as a Binding Corporate Code for such cases.

**Risk**

The draft Regulation already goes some way to incorporate a risk-based approach. There are references to the "risks to the rights and freedoms of data subjects" and Article 33 identifies types of processing operation which "in particular present specific risks….." In those cases a mandatory Impact Assessment is required and there has to be prior consultation with the DPA where there is likely to be a high degree of risk.

But, there are two main problems here:

- Although important, the language of "risks to the rights and freedoms of data subjects" is insufficiently precise. It does not elaborate which outcomes the

law is seeking to secure or avoid. Nor will businesses easily know what, if anything, they should be doing or avoiding.

- The listing of "risky" types of processing is indicative, but does not sufficiently capture what actually are the risks to data subjects, nor allow for differing degrees of seriousness.

**Accountability**

How should Accountability be captured in legislative text?

A broad statement of the principle, backed up by Guidance from the Commissioner, could be adopted. This is the approach adopted in Canada, although the widely-praised Guidance has only recently been published. The explicit Accountability Principle reads simply:

> ***"An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles."*** *(see Annex 2 for full text of section 14 of PIPEDA)*

Article 22(1) of the draft Regulation is (by itself) also a simple, sound and flexible articulation of the Accountability Principle:

> ***"The controller shall adopt policies and implement appropriate measures to ensure, and be able to demonstrate, that the processing of personal data is performed in compliance with this Regulation."***

However, many of the obligations which then follow in Part IV are excessively prescriptive and burdensome and do not need to be imposed in all cases, especially where the risks are not serious. In particular, much of the following Articles, as drafted, could be withdrawn as mandatory provisions and replaced by less much prescriptive wording and by the new requirements proposed below.

| | |
|---|---|
| Article 23 | Data Protection by Design |
| Article 28 | Documentation |
| Article 30 | Security |
| Article 33 | Data protecting Impact Assessment |
| Article 34 | Prior Authorisation and Consultation |
| Articles 35-37 | Data Protection Officer |

**Outline of new requirements**

It is very doubtful that the Canadian approach of very simple legislative text, backed up by non-statutory Guidance would ever be acceptable for the draft Regulation.

It is proposed, therefore, to develop text on the following lines:

- All Controllers should be ready to demonstrate their policies and measures upon reasonable demand from a DPA;
- Where the processing involves a risky type of processing, an Impact Assessment should be carried out;
- A Binding Corporate Code, which meets certain standards, should be adopted as the principal instrument of Accountability where:
    1. the Impact Assessment indicates a high risk that non-compliant processing could present serious harm to data subjects; or
    2. the Controller otherwise knows, or should know, that there is a high risk non-compliant processing could present serious harm to data subjects.

**Risky types of processing**

The risky types of processing, requiring an Impact Assessment, are broadly those set out in Article 33 (2) as follows:

| | |
|---|---|
| (a) | Automated profiling |
| (b) | Information on sex life, health, racial / ethnic origin etc |
| (c) | Public surveillance |
| (d) | Large systems on children genetic data or biometric data |

**Impact Assessments**

The Impact Assessment should be internal and not have to be shared routinely with the DPA or approved. Otherwise, Assessments are unlikely to be frank, full or helpful. But they should be subject to disclosure, after due process, in appropriate cases of enforcement action and sanctions would be greater where there has been no Impact Assessment or it is inadequate.

**High risk of serious harm**

The risk test should be elaborated in terms of the likelihood of serious harm which could be presented. Harm could be Material (tangible) or Moral (non-tangible), could involve Denial of rights or could be Societal. The following formulation is proposed as the test:

".....***where the processing operations present a high risk of serious harm to the rights and freedoms of data subjects by virtue of their nature, their***

***scope or their purposes. Such harm shall include in particular outcomes or events which would foreseeably cause damage or distress:***

1. ***to the life and physical well-being of data subjects;***
2. ***to the liberty or freedom of movement of data subjects;***
3. ***to the livelihoods of data subjects;***
4. ***to the financial interests of data subjects;***
5. ***to the family life and social relationships of data subjects;***
6. ***to the reputations of data subjects;***
7. ***to the personal autonomy or freedom of data subjects as a result of unjustifiable intrusion, breach of confidentiality, discrimination or other interference.***

***Such harm shall also include:***

1. ***denying the rights of data subjects created by this Regulation;***
2. ***harm to the democratic values of a free society.***

**Binding Corporate Codes (BCCs)**

It is proposed that Binding Corporate Codes should be required where the risk of serious harm is high. BCCs are broadly similar in concept, status and content to Binding Corporate Rules which have been developed for international transfers. A Code must be legally binding, must be adequately certified and must be adequately publicised. As a comprehensive privacy programme (tailored and contextualized for the actual processing undertaken by the data controller) it will operate as a ***flexible*** instrument of Accountability. But each Code will have to incorporate the core policies and measures as stipulated in the Regulation. Without undue difficulty (though not attempted here) the Regulation could be amended so that a Binding Corporate Code could also operate as the Data Controller's Binding Corporate Rules for international transfers.

**Proposed legislative text**

Annex 1 sets out proposed Legislative Text for incorporation (with corresponding deletions) into the draft Regulation which seeks to capture the above approach.

[redacted]

CIPL

23 March 2013