
THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

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

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

January 2011

EU Commissioner Register ID No. 10515222865-37
1900 K Street, NW
Washington, DC 20006

Executive Summary

Two Priorities

1. Accountability is an essential instrument for effective data protection and enforcement. It reinforces – but does not replace – legally binding ways for ensuring respect for the fundamental right to data protection. It encourages organisations to adopt and demonstrate tailor-made policies, procedures and practices for fulfilling the Data Protection Principles. It is not a self-regulatory tool, but does provide substantial scope for maximising effectiveness and minimising the burdens - the “Holy Grail” for data protection.
2. We propose a new framework of Binding Global Codes to improve and streamline arrangements for international transfers. This involves a re-cast BCR process, based on the Accountability Principle, where bespoke Codes with binding effect will be used to demonstrate and ensure practical compliance with the Data Protection Principles on a worldwide basis. We develop this proposal in more detail in a separate Paper.

More generally....

A modernised European framework for data protection is needed to address the realities of the digital world of the 21st Century.

The Centre agrees that EU Data Protection Principles remain sound, but argues that reform must focus on implementation and practicalities. The current approach is widely seen as not effective as it might be, with too many uncertainties and excessive burdens.

The Centre suggests criteria for a modernised regulatory framework, based on clear objectives, real risks and well-balanced outcomes.

We strongly support the Transparency principle, but stress its limitations. We have severe doubts about the efficacy of EU standard-form Privacy Information Notices which will be so comprehensive, or so simple, as to be meaningless either way. A sophisticated approach is needed, based on “reasonable and legitimate expectations”, with more attention on mis-statements.

There must be clarity of objective with data breach requirements, close attention to practicalities and avoidance of “breach fatigue”.

We support efforts to simplify rights of access, rectification, erasure and blocking, but are sceptical about a simple “Right to be Forgotten”. More discussion is needed, probably focused on use restrictions.

Promoting the free flow of information is an important policy goal - globally as

well as within the EU internal market. Harmonisation must be based on common principles and objectives, avoiding both highest and lowest common denominators. Harmonising regulatory approaches, including robust education programmes, is as important as the substance of the law itself.

Welcoming the commitment to reducing the administrative burden, we support attention on Notification requirements which do not serve any useful purpose. We support a very simple registration system designed to increase funding for DPAs and provide them with channels of communication for enforcement and education.

We welcome the emphasis on Privacy Impact Assessments and “Privacy by Design”, but a cautious approach is needed which encourages their use as business processes without crude mandatory requirements. We take the same approach towards Data Protection Officers.

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 The Commission and many other commentators are already aware of the work on Accountability 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.

1.3 The Centre welcomes the European Commission’s Communication on “*A comprehensive approach to personal data protection*” which is an important milestone on the route towards improving the data protection framework at EU level. We especially welcome the Commission’s recognition that the challenges of technology and globalisation are now driving the need for reform with unprecedented urgency.

1.4 This Commentary is deliberately selective – not attempting to address every issue raised by the Commission, but instead focussing on key points

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

which we would be happy to elaborate through meetings or correspondence. Drawing on the Centre's activities and experiences in recent years, our **top priorities** are to build the case for a new regime for:

accountability as an essential instrument for effective data protection and enforcement; and

international data transfers, undertaken in accordance with the Accountability principle, which will achieve good standards of data protection on a world-wide basis.

The structure of this Commentary broadly follows that of the Communication itself, with a separate Paper setting out more detail on the proposed new approach to international transfers.

2. Principle and Pragmatism

2.1 Although some may argue that an entirely fresh start should be made with the regulatory framework, the Centre understands and generally endorses the approach adopted by the Commission. There is broad agreement across the EU institutions, and across wider informed opinion, that the Data Protection Principles “remain sound” and that the “highest priority” should be given to “ensuring respect for the fundamental right to data protection”. This reflects the much-increased public, political and commercial interest in privacy and data protection world-wide. Beneath some different language, there is in fact a surprising amount of common ground across the issues raised in the Communication and reforms now under active discussion in the USA, notably in response to thinking within the Federal Trade Commission and the Department of Commerce and at Congressional level. The Centre has provided considerable thought leadership into these debates and has deep insights into them. We would be happy to share this experience with the Commission if that would be helpful.

2.2 It is important that the reform agenda prioritises implementation and practicalities. Despite endorsement of the Principles, the current EU approach is widely seen as not effective as it might be, not least because of too many uncertainties and excessive bureaucracy and burden which can deter good practice. Only recently has it become widely seen that processing personal data properly involves much more than formal rights and duties and legal compliance. Good information governance is cultural and must also embrace corporate and employee behaviours, training and awareness programmes and acceptable deployment of technology. There has been a transformation since the Directive was adopted in 1995, with the majority of commercial organisations now driven by reputational, financial and other reasons for **wanting** to process personal data properly.

2.3 It is also welcome that the Commission in effect recognises that data protection now impacts on virtually every organisation of whatever size or

sector. With such a range of business types and business model, and such widespread use of technology, it is important to recognise that “One size cannot fit all” and to avoid approaches which are excessively prescriptive. Even the smallest organisation can now process vast amount of sensitive personal data. The digital age - with powerful devices, instant wireless, mobile and fixed communications, open networks, more effective search and analytical tools and ever-cheaper data storage capacity - creates seemingly endless opportunities to gather and interpret information about us, our activities and our preferences. Data about anyone can be easily copied and aggregated around the world across vast, interconnected networks.

2.4 The criteria for a modernised, 21st Century, regulatory framework for Europe are that the legislation should:

- be based on clear objectives which are focussed on real threats to fundamental rights and the risks of other personal or social harm;
- aim for outcomes which reflect social norms;
- ensure a good balance between the benefits and the harms of processing personal data;
- promote good practice, while imposing minimum standards;
- be cast in accessible and relevant language which will facilitate predictable and consistent results;
- avoid stifling innovation by being technologically neutral and future-proof; and
- be internationally compatible, or at least inter-operable.

2.5 A specific reform consistent with our overall approach and these criteria would be to exclude business contact information (names, office addresses, e-mail and telephone details) from the definition of personal data. This exclusion across the EU – as already explicitly provided in Spain – would immediately and significantly reduce the burden of compliance with little real cost to personal privacy.

2.6 It has been widely recognised that the Centre has provided and stimulated detailed thinking which shows how the Accountability Principle meets these aspirations with a flexible and effective tool to promote high standards. This can be secured through legislation with a focus on clear objectives and outcomes, with requirements and incentives to identify and address both general and specific risks in each case. This also helps DPAs to move increasingly to from *ex ante* to *ex post* approaches, making a reality of the “Selective to be Effective” mantra and prioritising their attention on the poor performers who ignore the fundamental right to data protection or do not take it seriously.

2.7 To summarise, the underlying goal for new legislation should be to pursue the “Holy Grail” for data protection of:

- **maximising effectiveness (in terms of both protection and free flows of information); and**
- **minimising burdens.**

3. Strengthening individuals' rights

Transparency

3.1 The Centre has always been a strong supporter of the Transparency principle and welcomes the Commission's commitment to it. It must be right that individuals should be as well-informed as possible about the processing of their personal data. We agree that this must involve the use of accessible and plain language, whether online or offline. This is important in both private and public sectors. In the former, information for consumers is an important driver and enabler of competition and promotes privacy as a competitive element. In the public sector, readily understandable information about the existence, nature and extent of the processing is vital to the State/Citizen relationship.

3.2 However, the goal for transparency must not be to place the burden for compliance on individuals. It is important to be aware of the limitations of Transparency. First, there is now ample evidence the "Notice and Consent" model of data protection regulation, which places a great burden on individuals to read and understand privacy notices, is not especially effective in practice, as shown by the overwhelming empirical evidence that individuals do not read – let alone respond to - Privacy Notices, especially if they are lengthy. The Centre's 2004 project on Layered Notices emphasised the need to ensure that individuals do not receive more information than they want or can digest. But, even with a Layered approach, the default position is likely to remain that even the simplest notices will not be read.

3.3 Second, we have severe doubts about the efficacy of EU standard-form "Privacy Information Notices". There are so many data controllers and processors, with such diverse goods and services, with so many different business models marketing to consumers with so many different characteristics and needs that – even if they could be drafted - any standard form notices will inevitably be so comprehensive, or so simple, as to be meaningless either way. One size cannot fit all. The Centre's 2007 White Paper, *"Ten steps to develop a multi-layered privacy notice"*³, undertaken in cooperation with the OECD, demonstrates the real difficulties of drafting Notices, even for specific situations.

3.4 These limitations do not make transparency irrelevant, but they do point to the need for a sophisticated approach. For example:

- There is no need for explicit disclosure of "obvious" information;
- The legislative priority should be on disclosure – preferably on a "just in time" basis - of any processing which goes *beyond* the "reasonable and legitimate expectations" of the individual;

³ (http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf)

- Consent should not be necessary except in unusual, novel or otherwise sensitive situations;
- In line with the Accountability principle (see below) the regulatory priority should be action against mis-statements - essentially Notices which are false or misleading when matched against reality;
- Data protection should learn and borrow from other areas of EU consumer protection (e.g. food labelling) and develop a “traffic light” regime to give people immediate reassurance or warning (and drive standards higher.)

3.5 Consideration could also be given to a “Use and Obligations” framework for implementation and interpretation of the EU Data Protection Principles in a manner that reflects and serves the way data is used and managed in the 21st century. This approach switches focus onto the way an organization **uses** data to determine its **obligations** towards data subjects and to determine the appropriateness of the data and its processing. Obligations include such matters as transparency (notice), choice, access and correction. The model also focuses on the internal steps an organization should take to minimise risk to both the organization and the individual — covering such matters as data minimisation (collection and use); data quality and integrity; data retention and security. More details were set out in the 2009 discussion document on “*The use and obligations approach to protecting privacy*”⁴.

4. Breach Notification

4.1 The Centre recognises the powerful pressures for a mandatory breach notification regime. In other jurisdictions, the experience has been very diverse - regimes can be effective, burdensome or ineffective. Much depends upon clarity of objective (e.g. deterrent, punitive or compensatory?) and how the practicalities are addressed. It is especially important to avoid “breach fatigue” and to address a range of key issues. What types of personal data should be covered or excluded? Which types of breach should be notified? How best to avoid expensive notifications where the harm is minimal? Who should be notified – regulators or individuals? How much detail? With what consequences? These and other issues are explored more fully in two publications from the Centre:

- *Do’s and don’ts of data breach and information security policy*⁵; and
- *Information Security Breaches - Looking Back & Thinking Ahead*⁶

5. Rights of access, rectification, erasure and blocking and the “Right to be forgotten”

⁴ http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf

⁵ http://www.huntonfiles.com/files/webupload/CIPL_Dos_and_Donts_White_Paper.pdf

⁶ http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf

5.1 The Centre is supportive of efforts to simplify rights of access, rectification, erasure and blocking and to make them more effective in practice.

5.2 However, we are both unclear and sceptical about the so-called “Right to be forgotten”. If this means more than the existing rights of erasure and blocking it would come close to “re-writing history” - i.e. bringing about changes to records about factual events. A widely-drafted provision extending to complete deletion of material which may be embarrassing or damaging could have dangerous cultural, political and human consequences and is anyway likely to be opposed by all those who support freedom of speech and press.

5.3 This is not to dismiss the idea of a Right to be Forgotten altogether. We recognise considerable interest and discussion around the subject which may have utility in some circumstances and with respect to some kinds of data. Deeper thinking and reflection are clearly required here. One promising avenue may be to introduce more limited restrictions and limitations which focus on the use, rather than the retention, of types of data. For example it may be acceptable to restrict the use of retained police records to police purposes, banning for example their release for vetting purposes. Other examples – though not easy to achieve in practice - would be a right to demand deletions from a social network site or a presumption against access by employers to such sites. In any event, any right to oblivion should not extend beyond personal data which is readily accessible in the ordinary course of business.

6. Enhancing the internal market

6.1 As data flows ever more freely, this is an important dimension – globally as well as within EU. Further harmonisation is very important and very welcome in principle as divergence between national laws is very burdensome.

6.2 But harmonisation, both within and beyond Europe, must not aim for highest or lowest common denominators, but rather on common principles and objectives. This is especially important if there is to be any meaningful regulatory control as more and more organisations embrace cloud computing and other activities beyond conventional geographical and jurisdictional boundaries. Harmonization would not be welcome if it were based on stringent procedural requirements that would impose significantly greater burdens in some Member States and/or exclude major trading partners in Asia and North America.

6.3 The Centre certainly agrees that higher priority should go on harmonising regulatory approaches in practice than on substantive laws. As well as ensuring that DPAs are adequately staffed and resourced, the new legislation should impose a duty upon them to develop and execute robust privacy education programmes aimed at controllers, processors and individuals.

7. Reducing the Administrative Burden

7.1 The Centre very much welcomes the Commission's commitment to reducing the administrative burden. As mentioned, the "Holy Grail" for data protection should be maximising effectiveness in practice whilst minimising unnecessary burdens.

7.2 We especially support the wish to revise and simplify the Notification requirements. These are seen as ineffective and expensive, particularly for companies needing to provide and update a mass of detailed information in different ways in up to 27 countries. Radical re-thinking is required as to whether Notification currently serves any useful purpose. The concept was originally designed in a different era when it may have made sense for the regulators be provided with details of relatively few processing activities, mainly on a small number of mainframe computers.

7.3 We welcome the suggestion of a new registration system. Our vision – whether registration is at pan-EU or Member State level - is that nothing more is needed from data controllers than basic details of corporate identity and a reasonable registration fee which could be kept by the DPA. This approach provides increased funding (which is unlikely to come from public funds for the foreseeable future) **and** enforcement and educational channels of communication for DPAs. This would reinforce the Commission's calls for better resources and for more efforts at awareness-raising.

7.4 As the Article 29 Working Party has effectively recognised, the Accountability Principle – elaborated below – makes it easier to switch from Notification to Registration. It is more effective, more efficient and less burdensome to hold data controllers themselves accountable for complying with data protection requirements in practice than to impose a bureaucratic requirement to notify details of processing in advance and expect over-burdened DPAs to spot any problems. It may be necessary to reinforce a Registration system with powers (to the extent that they are lacking) for the DPA to demand details of processing from a data controller and to inspect processing in particular cases. This approach would be another desirable step towards "ex post" enforcement and would bolster new emphasis on targeted enforcement.

8. Enhancing Data Controllers' Responsibility / Accountability

8.1 The Centre welcomes the emphasis in the Commission's Communication on policies and mechanisms for ensuring compliance. As pointed out above, getting data protection right involves much more than legal compliance with formal rights and duties. Good information governance is cultural and must embrace both the awareness and behaviours of data controllers and their management and staff and how they use technology.

8.2 We especially welcome the reference to the Accountability Principle in this context, but this needs to be further developed. The papers emerging

from the Galway and Paris projects have already been mentioned and contain much material suggesting approaches (especially in relation to international transfers) which would be both effective and widely welcomed. The Article 29 Working Party's *Opinion 3/2010 on Accountability* is a further valuable contribution⁷. One very important point to make here is that the Accountability Principle is **not** a matter of self-regulation. It 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.

8.3 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.

8.4 Although the greatest and most sophisticated opportunity to put the Accountability Principle into legislative effect arises in the context of international transfers (see below), a more general obligation on all data controllers to demonstrate their approach to compliance can also be envisaged. But this must be seen – as did the Article 29 Group - as a means of **reducing** the administrative burden, not just a matter of “aiming not to increase the burden”. In this respect we felt that the Commission’s Communication is distinctly unambitious. The scope to abandon Notification requirements is one example where the burden can be reduced; another is the potential for more flexible sanctions where companies can demonstrate their compliance efforts.

9. Privacy Impact Assessments / “Privacy by Design”

9.1 Our support for the Accountability Principle means that we also welcome the Communication’s emphasis on Privacy Impact Assessments and the use of “Privacy by Design”. These are both elements of an accountability programme, which encourages organisations to identify and manage risks and to take a holistic approach to the deployment of technology.

9.2 The risks arising from processing personal information include:

⁷ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

- threats to fundamental rights and freedoms
- harm to individuals – economic, social, autonomy/dignity
- harm to organisations – reputational, financial, operational
- harm to society – relationships, trust, social stability.

9.3 Privacy Impact Assessments have rapidly become seen as the optimum way of identifying and addressing privacy risks by reference to their seriousness and likelihood. We support the use of PIAs by accountable organizations to discover and mitigate risk. However, there is a global discussion about using PIAs as a transparency device and a cautious approach is necessary. PIAs should be encouraged selectively, and with incentives, and not imposed universally. If companies were required to make all PIAs public, their effectiveness as a internal risk management device would be reduced.

9.4 We also welcome in principle the support for the “Privacy by Design” concept as a business process. In 2009 the Centre co-authored *“Privacy by Design: Essential for Organizational Accountability and Strong Business Practices”*⁸, which the Commission may find helpful. We believe that the concept should be actively encouraged, but again it is hard to envisage how it could be universally imposed. We recognise, however, that much will depend upon the precise legislative drafting and will respond to any specific proposals in due course.

9.5 The Centre is supportive of the role of Data Protection Officer. If there is to be corporate accountability, it follows that there need to be personal accountabilities and responsibilities inside the organisation. We have reservations, however, about the possibility that (as in Germany) the role should be made mandatory for organisations above a certain threshold. The main risk is that the appointment of a DPO becomes formulaic, resulting in appointees who (though notionally independent) lack real power and influence. It is striking that Chief Privacy Officers who have been appointed on a voluntary basis tend to operate at a much more senior level and have achieved strong strategic influence⁹. An obligation to appoint a DPO with standard-form functions could easily become an intrusive burden with no real benefit.

10. Encouraging Self-Regulatory Initiatives and Certification Schemes

10.1 Codes of Practice are superficially welcome, but a cautious approach is needed. In fact, there is a spectrum of different types of “self-regulation”.

⁸ http://www.hunton.com/files/tbl_s47Details/FileUpload265/2911/Privacy_by_Design_Abrams.pdf

⁹ If desired, the Centre could arrange for the Commission to receive copies of the IAPP’s 2010 Surveys of Role, Function and Salary for both European Data Protection Professionals and Global Privacy Leaders.

“Pure” self-regulation, with no reference to the legal framework, is not binding and brings risks of ineffectiveness, anti-competiveness and/or unfair advantage to companies who choose not to self-regulate. At the other extreme, there is nothing distinctive or valuable about so-called self-regulation which is externally imposed and scarcely differs from legal requirements.

10.2 We prefer the approach of “Co-Regulation”, where there is a clear and binding legal framework of principle which both requires and encourages companies to decide and demonstrate how they achieve the desired outcomes in their own way. At domestic and international level, this is one of the main attractions of the Accountability Principle – minimum imposed burden and maximum effectiveness in practice.

10.3 The Centre is pleased that the Commission will be exploring the feasibility of Certification schemes. Validation and certification issues formed a central part of the Paris phase of Accountability project and Commission may find it helpful to refer to the resulting report on Demonstrating and Measuring Accountability¹⁰. The key issues include: What is being certified? By whom? With what authority? and How meaningful will the “certificate” be for consumers? There are risks of high cost, limited practicality and threats to innovation which again point towards encouragement and incentive rather than compulsion. Drawing upon both successful and problematic schemes around the world, the Centre would be pleased to discuss the opportunities and the limitations of Certification schemes with the Commission.

11. The Global Dimension

11.1 We have already made clear that our top priority is to build the case for a new regime for international data transfers, undertaken in accordance with the Accountability principle, which will achieve good standards of data protection on a world-wide basis.

11.2 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. 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. The result is the paradox that substantial resources are expended by some organisations trying to “get it right” whilst there is unmeasured non-compliance by other organisations which ignore the requirements.

11.3 We therefore wholeheartedly welcome the commitment to “improve and streamline” arrangements for international transfers. We see this as by far the

¹⁰

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

most pressing priority for reform and are aware that other studies have reached the same conclusion. We consider that the most promising way forward is to build on the Binding Corporate Rule (BCR) approach. Reform is needed which will:

- establish a clear legal foundation for a BCR-type process;
- ensure that high standards of data protection are achieved globally in practice;
- be truly scalable to meet the needs of an integrated global economy which already has 63,000 recognisable multi-national companies and millions more SMEs which are regularly transferring personal data internationally;
- not place unrealistic demands upon over-stretched and under-resourced DPAs

11.4 We consider that “**Binding Global Codes**” (BGCs) are the best way forward. This approach is a re-cast BCR process based on the Accountability Principle, but scalable and without the current (but inevitable) delays and bureaucracy associated with BCRs. The BGC proposal allows and incentivises 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 on a worldwide basis. The Code must meet minimum requirements and 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 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 on action against false or misleading privacy statements.

11.5 A separate Paper which we are submitting simultaneously to the Commission sets out our analysis and concrete proposals in more detail, with specific legislative proposals.

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.