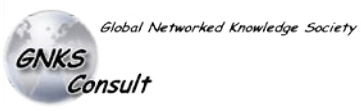
Review of EU Data Protection Directive: Summary

NEIL ROBINSON, HANS GRAUX,
MAARTEN BOTTERMAN, LORENZO VALERI

Prepared for the Information Commissioner's Office



May 2009

Foreword by Richard Thomas

We commissioned this study from RAND Europe as an objective, independent appraisal of the strengths and weaknesses of the Data Protection Directive. It is intended to provide food for thought and to stimulate debate. It is a not a blueprint for reform, nor does it contain the draft of a new Directive. It is intended to contribute to the shaping of future data protection law - it is part of a process that may take some years to come to fruition.

This report sets out the strengths of the Directive. The ones I wish to highlight are:

- It is comprehensive, broadly-drafted and sets out a basic framework of protection.
- It sets standards which are widely seen as "high" and has a strong Human Rights resonance.
- It gives people important and usable rights.
- Its principles have stood the test of time well and are flexible in their application.
- It is largely neutral in terms of technology.
- It has helped to harmonise DP rules across the European Union and provides an international reference model for good practice.

However, I see the main weaknesses of the Directive as:

- It is outdated, in terms of technology and regulatory approach.
- It has unclear objectives and insufficient focus on detriment, risk and practical enforcement.
- It is seen as bureaucratic, burdensome and too prescriptive. It focuses on "how" organisations should do things, rather than on "what" they should be achieving.
- It is not clear how much choice and control individuals should have, with regulators sometimes applying the law in a paternalistic way.
- Prescriptive criteria for processing personal data have become a rigid control mechanism. Much effort is devoted to the artificial justification of otherwise unobjectionable processing.
- Its scope is becoming increasingly unclear, for example in on-line and surveillance contexts.
- Its international transfer rules are unrealistic against a backdrop of high-volume, globalised data flows.

21st century themes for regulating the privacy and integrity of personal information must involve greater emphasis on trust, confidence, transparency, governance and accountability. Privacy and safeguarding information have become major reputational issues for businesses and governments. The European data protection community must become more aware of the pressures and changes inside China, India, USA and elsewhere in the world. It must, for example, see the APEC Privacy Framework as a source of new thinking, not as a competitive threat.

My six years as Information Commissioner have given me the opportunity to reflect on the challenges facing us and to identify the main themes which I consider to be essential in sign-posting the way to "Better Data Protection".

I start with the need for law that genuinely addresses risks to individuals, in terms of its rationale, content and implementation. As well as recognising the risks to fundamental rights and freedoms, the law must address the specific harms which can be caused by personal information being disclosed to the wrong people or used in unacceptable ways. It must also recognise that society suffers where

the improper use of personal information results in unwarranted intrusion into private lives or excessive governmental or organisational power.

Despite cultural and other differences, there is in fact significant agreement about the content of internationally accepted standards. I urge an approach, perhaps re-stating familiar concepts, including purpose limitation, security and access rights, which could bring the world closer to Europe and Europe closer to the rest of the world.

A vital theme is accountability. Primary responsibility must be placed on organisations to get it right and they must be held to account if they get it wrong. Organisations must deploy the right technology and have a privacy-by-design approach at the heart of their plans. This also depends on data protection becoming a top-level governance issue. Data protection is too important to be left to experts or to middle or junior managers.

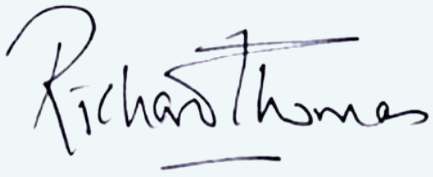
There must be more emphasis on the benefits of maximum and genuine transparency. There is scope for trust marks, accountability agents and perhaps self-certification. Improved Privacy Notices must get the right information to the right people in the right language at right time.

Commissioners must be strategic and enforcement must be improved. We have to set priorities and be selective in our different roles as teachers, ombudsmen & policemen. Commissioners must be well equipped to monitor and challenge organisational conduct, especially if things do go wrong. There must be meaningful sanctions, especially for deliberate or reckless failures.

Finally, there is now a pressing need to modernise the data export rules. At the least, reform must ensure a genuine adequacy test – no longer a pedantic and artificial equivalence test preoccupied with legal texts. A more radical – but probably inevitable approach in the long run – would be to abandon the export rules altogether and simply make data exporters responsible for ensuring that the data is processed in compliance with international standards, wherever in the world the processing takes place.

The themes of the report were discussed at the European Commissioners' Spring Conference which my office hosted in Edinburgh in April 2009. It is too soon for any consensus as to whether or how EU data protection law should be changed, but Commissioners are united in wishing to play a leadership role in the debate. That conference concluded with the unanimous adoption of the Edinburgh declaration, which is printed at the end of this foreword.

I hope that the RAND Europe study will be seen as a fair and objective appraisal of the current state of European data protection law. Whether you agree with everything or nothing it says, I am confident that you will find it well-informed and thought-provoking.



Richard Thomas, Information Commissioner

May 2009

Information Commissioner's Office

Promoting public access to official information
and protecting your personal information

Conference declaration

European Privacy and Data Protection Commissioners' Conference Edinburgh, 23-24 April 2009

Declaration on leadership and the future of data protection in Europe

Europe has a long and proud history of data protection standards and legislation. Some of these have been amended over time and some will remain under review. Legislation always follows technological and societal advances and it is a challenge for data protection authorities to keep pace with these advances and apply legislation and develop policy in rapidly changing circumstances.

Data protection and privacy standards and legislation are also developing at pace in the rest of the world, and Europe has had a role in some countries by giving advice and assistance. While the various standards and legislation that now exist may differ in certain areas, they all have as the ultimate goal of protecting personal information and the rights and freedoms of individuals.

The conference commits to contributing to the development of data protection in Europe and to putting European experience to good use in the global debate on privacy and data protection. This includes better implementation and enforcement of the existing legal framework.

European Data Protection Commissioners are committed to providing leadership for the future.

Accordingly, the conference anticipates that Commissioners will contribute constructively to the different ongoing work and initiatives aimed at advancing debate on the future of data protection in Europe and in particular on the future legal framework.

The conference will continue to promote the need for high standards of data protection in all areas of life, in particular as regards developing technologies, the online world and law enforcement activity.

The conference encourages the development and improvement of comprehensive data protection legislation that will:

- guarantee and promote fundamental rights and freedoms;
- build on the existing Data Protection Principles;
- focus on effectiveness in achieving desired outcomes in practice;
- encourage organisations to adopt best practice, including privacy by design;
- address the risks of adverse effects faced by individuals and by society at large;
- avoid burdens which cannot be justified; and
- provide for effective enforcement.

The conference calls on all those involved in debates about policy and law on data protection and privacy to focus on the similarities of different regimes and frameworks rather than the differences, and to search for ways forward which promote global solutions. In providing European experience to the global debate, the conference encourages a spirit of co-operation that is fully in line with the promotion of fundamental rights and freedoms.

With this declaration, the conference acknowledges the evolving landscape of data protection and privacy both in Europe and beyond, and the need to continue our work to promote data protection and privacy standards while adapting to the world in which we now find ourselves.

Objective of the study

In July 2008, the Information Commissioner's Office (ICO) commissioned a review of the 1995 EU Data Protection Directive (95/46/EC, hereafter "the Directive"). In the 13 years since the Directive came into force, the world has seen dramatic changes in the way personal data is accessed, processed and used. At the same time, the general public has become increasingly aware of the potential for their personal data to be abused. Through this study, the ICO wishes to examine if the Directive is still an effective tool for the protection of personal data, and what possible advantages could be gained through any alternative approaches.

Research approach

Using a variety of research methods, including a review of relevant literature, interviews with 50 individuals and a scenario-based workshop, we examined the strengths and weaknesses of the Directive and its current application in practice.

Overall conclusion

Overall, we found that as we move toward a globally networked society, the Directive as it stands will not suffice in the long term. While the widely applauded principles of the Directive will remain as a useful front-end, they will need to be supported by a harms-based back-end in order to cope with the growing challenge of globalisation and international data flows. However, it was also widely recognised that more value can still be extracted from current arrangements. A lot can be achieved by better implementation of the current rules, for instance by establishing consensus over the interpretation of several key concepts and a possible shift in emphasis in the interpretation of others. Abandoning the Directive as it currently stands is widely (although not unanimously) seen as the worst option, as it has served, and continues to serve, as a stimulus to taking data protection seriously.

This overall vision is reflected in the report you are about to read. Based on our findings, we have formulated recommendations in line with this evidence.

Context

The privacy of individuals is affected by a number of intersecting drivers, including the need to process personal information for social and economic reasons, technological developments and trends such as the popularity of the Internet and globalisation. The delivery of e-Commerce and e-Government are becoming centred on personal information.

Individuals are often willing or can be persuaded to give out personal data in the expectation of receiving economic or societal benefits. Public and private sector organisations are happy to provide individuals with these benefits but, in order to do so, must be permitted to legitimately collect, transfer and process the information. Individuals have also started to collect, manage and use personal data in similar ways, for example through social networking sites.

Against this background, it seems that the impact of the Directive on European perceptions of data protection principles has been largely positive. It can be credited with harmonising and professionalising the main data protection principles within Europe, even if implementation still varies, as will be explored below. The Directive can also be credited with creating one of the world's leading paradigms for privacy protection, which has served as an inspiration to legal regimes outside Europe.

However, despite this substantially positive track record and general acceptance of the sound principles behind the Directive, certain aspects have been criticised. Criticisms from within the EU have often focused on the formalities imposed by the Directive (or by the transpositions thereof), and the economic costs of compliance and unequal enforcement. Non-European organisations tend to perceive the European regulations as somewhat paternalistic towards other and perhaps equally valid data protection approaches.

The interviews conducted for this study illustrated that differences in implementation were the result of a complex interplay of factors, including legal heritage, cultural and historical norms and the personal and institutional characters of the regulatory authorities.

Challenges

Within the contexts of rapid technological change and globalisation, a set of distinct challenges were identified:

- Defining privacy – when is privacy affected by personal data processing and when is it not, and how strong should the link between data protection regulations and privacy protection be?
- Risk assessment – can we predict how risky it is to provide our personal data to an entity or organisation?
- The rights of the individual in relation to the benefit of society – under what circumstances can personal privacy become secondary to the needs of society, considering the fundamental importance of privacy protection for the development of a democratic society as a whole?
- Transparency – personal data is everywhere, particularly online, and through technological developments such as ambient intelligence and cloud computing could become increasingly difficult to track and control. How can we be sure how and where it is being used?
- Exercising choice – many services are only provided after sufficient personal data is released, but if important services are denied when we are unwilling to supply that data, do we still have a real choice?
- Assigning accountability –who is ultimately held responsible and where do we go to seek redress?

Strengths and weaknesses

The study identified a number of strengths and weaknesses associated with the Directive. The main strengths were:

- The Directive serves as a reference model for good practice.
- The Directive harmonises data protection principles and to a certain extent enables an internal market for personal data.
- The principles-based framework permits flexibility.
- The Directive is technology neutral.
- The Directive has improved awareness of data protection concerns.

The main weaknesses identified were:

- The link between the concept of personal data and real privacy risks is unclear.
- The measures aimed at providing transparency of data processing through better information and notification are inconsistent and ineffective.
- The rules on data export and transfer to third countries are outmoded.
- The tools providing for transfer of data to third countries are cumbersome.
- The role of Data Protection Authorities (DPAs) in accountability and enforcement is inconsistent.
- The definition of entities involved in processing and managing personal data is simplistic and static.
- There are other minor weaknesses which add to difficulties in its practical implementation

Recommendations

Our recommendations stem from a broad (though not unanimous) recognition that although a lot can still be achieved in terms of better implementation and interpretation of current arrangements, as we move toward an increasingly global networked environment the Directive will not suffice in the long term. In light of evidence collected during the course of the project, we have formulated a set of practical recommendations for getting the most out of current arrangements, along with a proposed regulatory architecture which we consider would be better suited for the future.

To extract the most out of the current system, we propose that:

- Member States, facilitated by the European Commission, need to seek agreement on efficient interpretation, implementation and enforcement of the Directive, including encouraging the use of a risk-based approach, making non-notification the general rule rather than the exception, ensuring that Binding Corporate Rules (BCRs) can be more easily used to legitimise data transfers to third countries, improving accountability and helping data processors meet transparency requirements.
- The European Commission should improve the effectiveness of the Adequacy Rule and facilitate the use of alternatives to this rule – such as standard contractual clauses and BCRs.
- The Directive should be explicitly included in the list of laws to be reviewed as part of the Better Regulation agenda.
- The Article 29 Working Party should work towards clarifying privacy norms and standards, the role of "privacy-by-design" for new technologies and business models that will foster compliance.
- The London Initiative should develop a common enforcement strategy for independent supervisory authorities through a non-binding Memorandum of Understanding.
- The Article 29 Working Party should expand liaisons with business representatives, civil society representatives and Non-Governmental Organisation communities.
- Data Protection Authorities, with guidance from the European Data Protection Supervisor (EDPS), should be encouraged to develop more accessible privacy policies e.g. comparable to the Creative Commons model for intellectual property rights licences.
- Member States should work with consumer protection related organisations to institute a system of local level accountability agents to help individuals exercise their rights and act as a means to prioritise workload for DPAs.

An alternative proposed regulatory model

To make European governance architecture properly viable given international data flows, we also recommend that the upcoming 2009 Consultation considers an alternative proposed regulatory model, outlined below. This is based on:

1. **Defining high level Outcomes**
2. **Defining globally consistent General Privacy Principles ("General Principles") based on well-known existing data protection instruments such as the European Charter on Human Rights and the 1981 Council of Europe Convention No. 108;**
3. **Implementing tools and instruments to achieve these, and**
4. **Foreseeing effective enforcement measures to ensure accountability when the Outcomes are not met or the Principles are not respected.**

This will require the re-casting of the Directive to become an instrument clearly describing:

1. **Outcomes** in terms of expectations for stakeholders:

- Individuals – to retain clear and effective safeguards whenever personal data is processed, including via accountability of the data controller, thus contributing to the protection of private life. To have the choice to exercise significant control over their personal data, including by sharing personal data with trusted third parties or withholding it from them, but to be mindful of the implications of this in an information society.
- Public and private sector organisations – to be able to use personal data and derive economic or societal value as long as this remains aligned with the General Principles, in particular by processing data in line with the stated purposes, ensuring the legitimacy of their activities in accordance with applicable rules, and in the knowledge that they will be held accountable for non-compliance.
- Independent Supervisory Authorities (ISAs) – to act independently and equitably across both public and private sectors, but to do so in a way that is mindful of the realities of the use of personal data. To use enforcement where necessary both to shape good behaviour and obtain restitution for any harm.

2. Globally consistent **General Principles** concerning privacy protection:

- Legitimacy – defining when personal data processing is acceptable.
- Purpose restriction – ensuring that personal data is only processed for the purposes for which it was collected, subject to further consent from the data subject.
- Security and confidentiality – specifically by requiring the data controller to take appropriate technical and organisational measures.
- Transparency – that appropriate levels of transparency are provided to data subjects.
- Data subject participation – ensuring that the data subjects can exercise their rights effectively.
- Accountability – that those processing personal data would be held accountable for their actions according to the Outcomes.

The implementation or 'back-end' aspects, i.e. the processes to ensure that these General Principles are respected, should be delivered by other more suitable means, which may need to be created or defined by formal EU level implementing measures or locally at the national level. The selection of appropriate means for specific acts of data processing can be determined locally, either via national data protection rules (generic or sector/context specific) or via co-regulation (e.g. established via dialogue between ISAs and sectoral representatives). This selection should be based on considerations of risk, with more burdensome tools being used only when this is justified by the risk presented by specific acts of data processing.

Further discussion will be required to clarify how regulation can appropriately consider and address the presence of risk. Possible criteria or avenues for determining the risk involved in specific categories or acts of data processing include:

- the scale on which personal data is processed (e.g. more stringent requirements could be applied to the processing of personal data based on numbers of data subjects involved);
- the privacy sensitive nature of the data being processed, and more specifically whether the nature of this data causes it to be more likely to result in harm, considering the full context of the data processing (e.g. the processing of health-related information, racial information, etc) and
- the field of activity of the data controller, as a proxy for the risk of harm (e.g. financial services, health care, legal services).

While risk is often difficult to determine ex ante, the strength of a risk-based approach lies precisely in the need to evaluate how risk changes dynamically as data processing practices evolve (e.g. because of changes in the scale of data processing, or expansions to other fields of business). As practices change (and as risk changes), the measures needed to ensure compliance will evolve as well. In this way, a risk-based approach stresses the importance of implementing a sound data protection culture, rather than meeting one-off compliance formalities.

The need to appropriately consider risk as the predominant consideration in determining in what way the fundamental right to the protection of personal data as specified in the European Charter of Fundamental Rights may be best safeguarded supports this right without the imposition of inappropriate or disproportionate burdens. A risk based approach should thus not be interpreted as arguing for the application of regulations only when there is a sufficient risk of harm.

Data protection practices can thus be assessed on the basis of whether the desired Outcomes and General Principles are met, rather than on the basis of a process orientated review. Mutual acceptance of different instruments as viable routes to achieving the Principles and Outcomes would be required to mitigate the risk of fragmentation of the internal market (for instance, by one ISA refusing to accept an instrument considered as valid by another).

3. **Implementation measures** would include:

- Privacy policies – internally focused tools describing how an organisation intends to achieve the principles set out above and a clear means to provide for accountability.
- Privacy notices / statements – externally facing tools supporting objectives of transparency, these would alert individuals at an appropriate time and context as to how their personal data is being used.
- Chief Privacy Officers – this role may be identified as an alternative to a privacy policy, there mainly to provide for accountability within an organisation.
- Codes of Conduct – self-regulatory tools defining the common rules for similar types of organisation.
- Corporate Governance Codes – developed and published by the regulator, these might be non-binding set of rules for organisations to follow, where they must comply or explain why they do not.
- Privacy Reporting / Accounts – based on the likely risk, organisations might be compelled to produce data reflecting their use and incidents relating to personal information.
- Standards – providing for another aspect of accountability by allowing regular external review of processes and policies by third parties to ensure the organisation is living up to its own rules.
- Kite-marks / Trustmarks / Seals – a way for consumers to exercise their rights as an enabler of choice between those organisations that display a trust mark and those that do not.
- Privacy Impact Assessments – a way to assess a-priori the impact of certain measures upon individuals' privacy, formal and informal methods of conducting Privacy Impact Assessments support the same purpose of encouraging responsibility and respecting proportionality.
- Technology – a way to enforce policies or support compliance, technology may be used appropriately in the context of the greater objectives of the achievement of Outcomes by satisfying General Principles.
- Targeted information campaigns – to increase understanding of risks and issues regarding the use of personal data amongst individuals and public and private sectors.

Some of these tools will be more appropriate for either public or private sectors and ISAs might establish mandatory uses of some instruments for the public sector. The public sector might also be able to set an example in adoption of various instruments.

National legislation, along with cultural and political conditions, will play an important role in the implementation of these tools in the public sector.

4. To support these tools, **strong enforcement** will be necessary.

ISAs must be able to intervene when misuse has been identified, either pre-emptively, or after the fact when actual harm has occurred. In order to ensure effective and credible enforcement:

- Possible liabilities, sanctions and temporary measures should be clearly published.
- Criteria for determining fines should consider risk –for example, numbers of personal records involved, whether the incident involved actual harm, and if so, what sort of harm.
- Criminal sanctions may be considered for serious incidents or intentional misuse, to act as a deterrent and punishment.
- Alternative Dispute Resolution may also be considered, to permit easy and quick access to restitution or compensation in low level cases of misuse.
- Efficient enforcement can be improved through strategic partnerships and joint enforcement efforts between ISAs and consumer protection bodies, especially in countries where there is a stronger culture of consumer protection. This will improve coherence in protecting the individual, and will encourage compliance with data protection regulations to evolve into an economic differentiator.
- Ultimately, ISAs will need to act more strategically to achieve real outcomes rather than meeting targets for completed investigations.

All this indicates that ISAs, those organisations using personal data and individuals will need to assume greater responsibility for achieving the Outcomes. For their part, ISAs will need to adopt an approach that is less focused upon process and formality checking, but instead aims for more effective enforcement and ensuring accountability. Those using personal data will need to assume responsibility for making sure the measures they select to achieve the Outcomes are consistent with the level of risk that personal data is exposed to by their business activities. Individuals must also take more responsibility in the choices they make with their personal data.

The research for this study showed clearly that the success or failure of privacy protection is not principally governed by the text of legislation, but rather by the actions of those called upon to enforce the law. It cannot be stressed enough that supervisory authorities must be given an appropriate level of responsibility for this arrangement to work.

This document is a summary of a RAND Europe Technical Report TR-710-ICO available at http://www.rand.org/pubs/technical_reports/TR710/

The views expressed in this study are those of the authors and do not necessarily reflect those of the Information Commissioner's Office.

EUROPE

Westbrook Centre
Milton Road
Cambridge
CB4 1YG
United Kingdom
Tel. +44 (0) 1223 353 329
Fax +44 (0) 1223 358 845

37, Square de Meeus
B-1000 Brussels
Belgium
Tel: +32 (0) 2 791 7500
Fax: +32 (0) 2 791 7900