



Data Protection in the European Union - Promising Themes for Reform

Richard Thomas
UK Information Commissioner

European Privacy and Data Protection Commissioners' conference
Edinburgh, 24 April 2009

The Review of the EU Directive prepared for my Office by RAND Europe has been presented to participants at this conference as a draft. The presentation by Neil Robinson and Hans Graux has highlighted their main findings and short and long-term recommendations. Peter Hustinx has added some very perceptive and important observations. We plan to publish the final version of the RAND Report in May – shortly before the conference which has been convened by Commissioner Jacques Barrot. We have always been clear that the RAND study is intended to provide food for thought and to stimulate debate. It is not a blueprint for reform, still less does it contain the draft of a new Directive. We are equally clear that any reform will take many years, but the debate must start somewhere. That debate has started here in Edinburgh today. As the draft Edinburgh Declaration which will be discussed tomorrow makes clear, the fundamental role for Commissioners in this debate is that of Leadership.

As you know, I cease to be the UK Information Commissioner in June. I have been involved in many international conferences over the last six and a half years, but this will be my last. In my short presentation, I want to pick out some key conclusions from the RAND report which I think are of particular importance and then set out – very briefly – eight Themes which I personally consider to be essential in sign-posting the way to “Better Data Protection”.

I start with **Strengths**. As our draft Declaration makes clear, Europe has a long and proud history of data protection standards and legislation. Particular strengths can be summarised as follows:

- The Directive is comprehensive, broadly-drafted and sets out a basic framework of protection, drawing on OECD and Council of Europe approaches.
- It sets standards which are widely seen as “High” and has a strong Human Rights resonance, with sharp focus on fundamental rights’ and freedoms.
- It has given people important and usable access and other rights.
- The basic Data Protection Principles have stood the test of time well and are flexible in their drafting and application.
- The Directive seeks to be largely neutral in terms of technology.
- The Directive can claim significant success in harmonising DP rules and promoting an internal market across the European Union.

- It provides a reference model - or at least a starting point - for good practice, no least outside the European Union.
- There have been some significant international successes – for example with SWIFT and with pressure for search engines to reduce their retention periods.

But we must not allow complacency to cloud our judgement. It is impossible to deny that there are weaknesses too. The Directive has sharp critics and there are real risks that others will articulate weaknesses with a shriller tone than mine and press for change which will not be welcome. That is why I place so much emphasis on Commissioners asserting Leadership and championing improvement. As Peter Schar said recently: “We must be in the driving seat.” If we do not lead with an honest and constructive approach, others will step into the vacuum.

My approach is to divide the weaknesses into the general and the specific. I see the **general weaknesses** – which apply to both the words of the Directive and to the implementation of the law in practice – as follows:

- The approach is now outdated – in terms of both technology and modern regulatory approaches. Technology has moved on massively in the last 20 years. It is a “Mainframe Directive”.
- But regulation has also moved on. “Good” laws are those which:
 - are clear about their objectives;
 - are focussed and proportionate in the problems they address;
 - provide incentives and deterrents for maximum “self-enforcement” by organisations to achieve standards at or above the minimum level;
 - have effective enforcement mechanisms; and
 - avoid financial and operational burdens which cannot be justified.
- I fear that the Directive has insufficiently clear objectives and insufficient focus on detriment, on risk and on enforcement in practice.
- It is also widely seen as excessively bureaucratic and burdensome, and too prescriptive. Detailed rules tell organisations “How” to do things, with less attention to “What” they should be achieving or their own responsibility for achieving it.
- I worry that Data Protection has – perhaps inevitably - been “captured by experts”. Data protection is far too important to be left in the hands of experts talking to each other and writing learned papers which outsiders cannot understand. Data protection must not become remote from citizens, and certainly not (as can happen) something they regard as causing them problems.
- At the same time, more clarity is needed about much choice and control is available to individuals. Apart from the vulnerable, the law should avoid any paternalistic suggestion that we know better than citizens what is in their best interests.

To sum up, at the general level, the current arrangements can be portrayed as “Words, not Actions” and “Not sufficiently effective in practice”.

Turning to some of the **specific weaknesses**:

- Notification is a poor and burdensome tool for transparency
- In the era of extraordinarily high-volume data flows, the need for prior authorisation or approval is an old-fashioned, but also unrealistic, regulatory tool.
- Prescriptive criteria for processing personal and sensitive data have become a rigid control mechanism, with much time and energy devoted to artificial justification for otherwise unobjectionable processing.
- We are all aware that some of the concepts and definitions - such as the controller / processor distinction - are static and in need of fresh thinking.
- There are uncertainties about scope, especially in the on-line and surveillances contexts.
- There is an obvious need for an integrated approach as between 1st and 3rd Pillar issues.
- The data export rules are especially outmoded and unrealistic.

My next point is neither a Strength, nor a Weakness. But it is fundamental that we conduct discussions in the **global context**. We must be realistic:

- Globalisation is no longer a word, a slogan or spectre to fear. It is simply the Reality – in economic, technological, and social terms.
- We need to recognise and welcome 21st Century global themes for regulating the privacy and integrity of personal information where
 - there is new and heavy emphasis on Trust, Confidence, Transparency, Governance and Accountability; and where
 - privacy and safeguarding information have become major reputational issues for businesses and governments.
- We must – without prejudice or false assumptions - become more aware of the pressures and changes inside China, India, USA and elsewhere in the world.
- We must see the APEC Privacy Framework as a source of new thinking, not as a competitive “threat”. We must focus on the 80% which we have in common with our international colleagues, not the 20% where we differ.

Against that background, I turn now to the **eight Themes** which I personally consider to be essential in sign-posting the way to “Better Data Protection”. Before saying a few words about each, I can summarise them as follows:

1. Explicit focus on outcomes - reducing risks of adverse effects to (a) Individuals and (b) Society
2. Clear Standards which organisations must achieve

3. Hold organisations to account for failure to achieve Standards in practice
4. Genuine transparency
5. Convert Notification to Registration
6. Greater clarity for Commissioner role
7. Improved Enforcement
8. Modernise export rules

I start with the need for a more explicit focus on outcomes which address **risks to individuals**. The need for such focus applies to rationale, content and implementation. The starting point must be the risks that the fundamental rights and freedoms of each individual may be reduced or threatened. A risk or harm based approach is not in any way incompatible with emphasis on fundamental rights and freedoms. An individual's dignity or privacy, for example, can be just as much at risk as more tangible possessions or benefits such as loss of money or career. Loss of informational self-determination is just as much a harm, detriment or adverse effect as loss of property. But it is easier to understand why data protection matters if we can clearly identify and articulate **all** the risks which may materialise if the law is not effective in practice. We therefore need laws which stop all types of harm which can be caused if personal information is:

- inaccurate, insufficient, or out of date
- excessive or irrelevant
- kept too long
- disclosed to wrong people
- used in unacceptable or unexpected ways
- not kept securely

In exactly the same way, there needs to be explicit focus on the **risks to Society** at large. We all suffer if fundamental rights and freedoms are placed at risk. One individual may not suffer if another's rights or freedoms are threatened or denied, but the harm is experienced by Society. And this can happen, sometimes more tangibly, where improper use of personal information results in:

- excessive intrusion into private lives
- loss of personal autonomy or dignity
- arbitrary decision-making, stigmatisation or exclusion
- excessive governmental or organisational power
- a climate of fear, suspicion or lack of trust.

The content of the substantive law is much less controversial than its application. Here – despite cultural and other differences in some regions and more widespread differences of precise language – there is in fact significant agreement about the content of **internationally accepted standards**. I applaud the efforts of our Spanish colleagues to see whether a genuine international vocabulary can be secured. The rest of the world needs to come closer to Europe and Europe needs to get closer to the rest of the world. I urge a clear approach, perhaps re-stating familiar concepts in language which is as simple as can be achieved, for example:

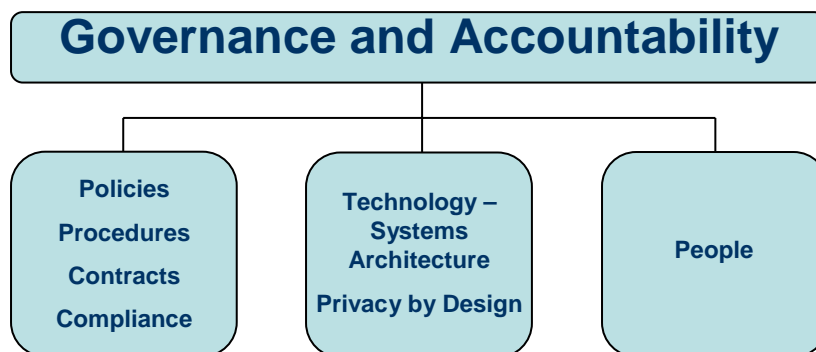
- Collection, use or disclosure based on consent, legal requirement or within the reasonable expectations of individuals.
- Duty of care for integrity of personal information
- Purpose limitation / data minimisation / proportionality
- Transparency of processing
- Limitations on retention and onward disclosure
- Accuracy
- Security
- User-friendly rights to access to own information
- Effective arrangements for compliance, complaint and redress

My third Theme is an area where the Directive is weak: **Accountability**. The need for greater accountability will be explored in more detail at the conference which Billy Hawkes is hosting in Dublin next week. Basically it means that:

- Organisations must be held to account, for fulfilling privacy policies, which meet minimum legal requirements, but in ways best-suited to the organisation
- Primary responsibility must be placed on organisations to get it right and they must be held to account if they get it wrong.
- Data Protection must become much more of a top-level Governance issue. Just as it is too important to be left to the experts, it is too important to be left to middle or juniors managers.

This diagram demonstrates what I mean by true accountability. We must make sure that responsibility for the right approach to safeguarding Reputation and meeting Regulatory requirements rests at the very top of the organisation – with Chairmen, Chief Executives and Management Boards. Things go wrong if data protection is left in just one of these boxes.

Reputation and Regulation matters for the Board



Of course the paperwork must be right in terms of the right policies, procedures, contracts and compliance arrangements. That is largely the domain of lawyers, compliance officers and specialist data protection officers. It has indeed been the central focus in many organisations. But is not enough. In addition, the right approach needs to be taken to the organisation's technology – whether deploying the appropriate level of encryption or using privacy enhancing technologies. The IT specialists usually know only too well the full capabilities of the IT and also the full consequences of losing control. Often others – including their bosses – are sadly ignorant or wrongly assume that all is well. But it is not enough to trust the IT Department look after data protection. Privacy by Design needs to be at the heart of architectural plans, not bolted on once systems go live and problems come to light. But full accountability also means that the people who run organisations at every level – often in reality the weakest link – actually safeguard the information of customers in practice. This means awareness and operational training and the right cultural atmosphere. But - again - data protection is too important to be left to training from the Personnel or Human Resources Department. They must be involved, but only as part of the wider team.

So there must be a holistic and ethical approach. There must be someone at, or near, the top who is directly accountable for pulling together the right paperwork, the right technology and the right people. And new laws must hold organisations accountable for getting the right results.

Time prohibits a fuller exposition of my remaining Themes, but they are largely self-explanatory:

There must be more emphasis on the benefits of maximum and **genuine transparency**, for example:

- Privacy by Design and the use of published Privacy Impact Assessments.
- There is much more scope to encourage and require organisations to adopt Privacy Policies, make them easily available and – of course - hold them to account for fulfilment.
- There is more scope for trust marks, accountability agents and 3rd party certification.
- More controversially, perhaps, we can envisage greater use of self-certification.
- And we must improve the use and content of Privacy Notices, getting the right information to the right people in the right language at right time.

Next, I urge **abandonment of Notification in favour of Registration**. Little transparency or other purpose is served by giving Commissioners details of processing. That harks back to mainframe days. The situation is made much worse by sharply different requirements in 27 different countries. True transparency about how data is processed should be primarily directed at the

individuals affected, not the regulator. All that is needed centrally is registration of very basic corporate details which will ensure:

- easy identification of corporate entities for efficient and effective enforcement when necessary; and
- electronic and other communication channels for Commissioner advice and messages.

In the UK – and perhaps elsewhere in future - we also welcome the fee which comes with each registration which funds all our data protection activities and improves the Commissioner's constitutional independence.

The next two Themes run together. **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.
- There must be improved enforcement with Commissioners monitoring and challenging organisational conduct – holding to account, especially if things do go wrong.
- And there must be meaningful sanctions, especially for deliberate or reckless failures.

Commissioners do not have to have a monopoly of enforcement. Indeed that can take responsibility away from data controllers. Controllers must have clear and direct liability and consideration should be given to group actions.

My final promising Theme for reform merits a conference of its own. There is now a pressing need to **modernise the export rules. At the least, reform must ensure:**

- A genuine Adequacy test – no longer a pedantic and artificial Equivalence test preoccupied with legal texts.
- The focus should on corporate practice, not theoretical rules – for example real redress for individuals, not rarely-enforced 3rd party rights under contracts.
- And if Binding Corporate Rules are to take off seriously there must be scope for certification by third parties other than Commissioners who are already totally swamped by the tiny number of current applications.

A more radical – but probably inevitable approach in the long run – would be to abandon the Article 25/26 construct altogether and simply make data exporters responsible, but properly accountable, for ensuring that the data is processed in accordance with the international standards anywhere in the world. In other words, place the burden where it belongs - on the corporate shoulders of the exporter.

CONCLUSION

Thank you for listening. The RAND team have given us all much to digest. Other speakers will doubtless make interesting contributions of their own. Next month's conference in Brussels will take debates one stage further. There is a long road further ahead after that. Whether you agree with everything or nothing that I have said – or somewhere in between – my only wish today is to stimulate thinking and talking.