

## Crispin Blunt speech, DP Conference

### Introduction:

- Ladies & gentlemen, I would like to thank the Secretary-General of the Council of Europe for inviting me to speak before such a distinguished audience of Data Protection experts. I understand that there has been considerable discussion in the past few days in the conference room, and I am pleased to be given the opportunity to contribute further to this debate.
  
- Data Protection, might on first glance, appear a subject reserved only for IT sophisticates, but in fact it raises some fundamental questions about how we interact with private and public organisations – as well as with each other - in a rapidly changing world.
  
- The conference comes at a key time with the Council of Europe modernisation programme on Convention 108, the long-awaited publication of Data Protection proposals by the European Commission and the marking of Data Protection Day itself which - although is officially tomorrow (28<sup>th</sup>) - I am very pleased to mark today without impinging on your weekend.
  
- I also welcome the opportunity to represent the UK Chairmanship of the Committee of Ministers of the Council of Europe today. One of the UK's priorities for the Chairmanship is internet governance, and we strongly support the work of the Council of Europe in this fast-developing field. While data protection is a longer-established and broader subject, it is also, of course, a key aspect of internet governance.
  
- As we mark the occasion of Data Protection Day it is worth recognising the considerable achievement made by the Council of Europe in setting the benchmark for universal data protection standards. The inception of Convention 108 in 1981 marked the formulation and agreement to a number of core principles which have governed the protection of up to 800

million individuals with regard to automatic processing of personal data, and in doing so reconciling the free flow of information with privacy and data protection concerns.

- It has provided safeguards concerning the lawful and legitimate collection and processing of data, while imposing strict conditions for the use of information and guarantees of information and access for data subjects. Not only that, it goes beyond the European stage, in that it remains the first and only binding international legal instrument with a worldwide scope of application in the field of data protection. It is open to any country, including those which are not members of the Council of Europe. So far, Convention 108 has been ratified by 43 European States. And, in June 2011, the Committee of Ministers invited the first non-member state, Uruguay, to accede.

#### Why change:

- While it is right to celebrate past achievement we must also recognise that the world and the society we live in is rapidly evolving. The extraordinary pace of technological innovation, increasing global interdependence and the growing transfer of people and information within and across borders presents a significant and unprecedented challenge. No one can be sure what further changes may be around the corner, but we must be proactive in taking the right steps now to create an environment in which: business and enterprise can prosper; the police and judicial authorities are able to protect and serve the public effectively; and where individuals can be confident that their privacy, safety and freedom will be safeguarded.
- In the current environment of cloud computing, social networking and other forms of new technology, individuals - both in Europe and beyond - want to be confident that their privacy, safety and freedoms are strongly protected. To this end, they want to know their personal information is

safe and secure and not exposed to criminal activity or mechanisms of unnecessary state interference, whilst being able to share the value and benefits of the data held. None of us would disagree that the world has changed immeasurably in the last thirty years and that improvements to the current data protection regime are needed if we are to provide the right safeguards to protect our citizens from harm while ensuring business and innovation is not stifled by excessive regulation. The focus of current debate is how we best achieve this ambition.

- So one of the key questions to ask in respect of data protection is: what is the most effective framework for operating a robust system that puts data subjects at the heart of its thinking?
- I believe that the starting point for an effective system of data protection is that the use of personal data should be fair; lawful; accurate; secure; and that data itself should be kept for no longer than is necessary. These are the principles that formed the basis of the first data protection laws in the UK some thirty years ago. I believe they are still relevant today. These principles transcend technological and political developments and their strength lies in their generality, in that they can be applied in different contexts irrespective of political and technological change. Where those principles are inadequate or no longer effective, we should rightly look to revisit them.
- But, we should be mindful about being excessively prescriptive and failing to take account of the subtle nuances, both legal and practical, in introducing changes to data protection rules across member states. Simply imposing detailed prescription is unlikely to make our citizens safer or freer. In fact, such a regulatory straight jacket runs the risk of doing the opposite and tying the hands of individuals who seek to protect us from harm.

### Provisions of Convention 108:

- With this challenge in mind, I welcomed the approach taken by the European Ministers of Justice at their conference in Istanbul in November 2010 in calling for the modernisation of Convention 108. I similarly endorse the consultative approach taken with governments, data protection authorities, NGOs, the private sector and professional associations. The strength of this approach lies in the transparent and evidence-based nature of the process, and reflects the approach the coalition government has taken to introducing substantive policy change in the UK in the fields of criminal justice reform, health, education etc. It is absolutely right that we tap into the expertise and knowledge of those most affected by any proposed changes to the data protection model.
- The UK government supports this approach, and in particular the principle-based, but flexible way of delivering change to the data protection regime. Indeed, we conducted our own call for evidence with key stakeholders and interest groups in 2010. The main message that came out of the consultation was one which supports a non-prescriptive approach that recognises shared values but rejects a one-size-fits all way of delivering change. Each of our countries has particular cultural and legal identities which define who we are, and in introducing change we should be sure that change is complementary and not contradictory.
- My colleague, Ken Clarke, Secretary of State for Justice made a speech last year in which he drew a rather apt 'comparison with the very idealistic proponents of Esperanto. It's a fact of life we live in a multi-lingual world. But, as he argued, whatever the inconveniences this brings, it's a challenge that is never going to be solved by inventing and adding a universal additional language. Indeed, the one solution guaranteed not to work faced with a multiplicity of languages is an additional tongue that no one speaks. What we need instead is to improve our ability to understand each others' languages better.' The analogy with the

changes to data protection rules is that we should look to better understand each other and our respective laws rather than unpicking enduring principles and introducing an entirely new, and quite possibly impractical regulatory framework.

- Let us briefly touch on the provisions proposed for consideration by the Council of Europe. The focus is rightly on the need to deal with the significant challenges for privacy that arise from the use of new technologies. From the public consultation there already appears to be wide consensus on the objectives to be pursued, namely:
  - o To maintain the Convention's provisions at principle-level, to be complemented by texts which are tailored to sectors by way of recommendations or guidelines;
  - o To ensure for consistency and compatibility with the legal framework of the European Union;
  - o To maintain technologically neutral provisions;
  - o To reaffirm the Convention's potential as a universal standard
  
- In this regard, I strongly welcome the convention philosophy, one of general principles which are simple in their interpretation, and allow member states a measure of discretion when implementing through their national legislation.

#### EU Data Protection Instruments (Regulation and Directive)

- I say all this conscious that at the same time as the revision of Convention 108 has begun, the European Commission has generated and on Wednesday [25<sup>th</sup> January 2012] published proposals on two new data protection instruments. The Regulation proposed by the Commission will replace the existing Data Protection Directive (95/46/EC) and will apply across the board to regulate data protection in general, apart from for the purposes of law enforcement. The Regulation will cover all data

controllers in the public and private sectors, with exemptions where these are needed for journalism, official records, research and other vital areas.

- The draft Directive we have before us will replace the existing Data Protection Framework Decision (DPFD), which covers the former third Pillar (Police and Criminal Justice). This will be aimed primarily at “competent authorities” i.e. police and other law enforcement bodies as well as bodies responsible for judicial cooperation.
- The revision of these instruments is a landmark for data protection. The proposals are far-reaching and will provoke widespread discussion about their merits. Given the short time elapsed since their publication, I would like to touch on just one component of the proposals as I consider it to have a broader resonance on the question of how we best protect privacy and freedom while recognising the harm that can result to citizens from a failure to share information. And what’s more it speaks directly to the debate on how best to effect workable change across EU member states with varying legal and procedural rules.
- That is the so-called ‘right to be forgotten’, and it’s an area where I would sound a note of caution. The central provision of the ‘right to be forgotten’ is that data subjects have the right to request the erasure of data about themselves if it is no longer being processed. At first glance, the aim of reducing excessive data retention and giving individuals greater autonomy over their personal data seems commendable. But we must ensure that its effects are both proportionate and workable
- Health records is one example, where my fear is the proposed changes could critically undermine what the Health Service is trying to achieve. Similarly, without data regulation on credit histories, we run the risk of limiting loans and mortgages, potentially to those most in need. Businesses should have the right to conduct due diligence to assess the merits and financial means of an individual. This isn’t the time to be

undermining effective and responsible lending or hampering businesses taking legitimate measures to prevent financial crime

- On a more fundamental level, in a digital age where data is transferred and replicated in a matter of seconds how would this actually work in practice? The proposal we've seen rightly provides carve-outs for freedom of expression, scientific research and other important areas. We welcome these and will examine them closely. But my concern is we may be running the risk of setting the standard so high, that we are unlikely to ever achieve a workable model.
- In my view, it should be the legitimate right of Member States to decide when to use and share data to keep their citizens safe, particularly in detecting crime and preventing terrorism. London will host the biggest international event on the calendar this summer with the hosting of the Olympic Games and the public at large, both British national and guests from around the globe rightly expect to be able to enjoy this celebration of sporting excellence in the knowledge that the relevant authorities will take the necessary measures to ensure their safety [although instruments will not be implemented by this time, the principle remains]. We are naturally still assessing the implications of the directive and the regulation. But imposing a new regulatory framework that potentially imposes a significant burden on law enforcement agencies runs the risk of undermining their ability to act decisively to prevent harm to the public. We believe this maybe a step too far.
- Similarly, the UK is keen to ensure that any new proposals do not place too onerous burdens on small and medium enterprises (SMEs). We want to avoid SMEs from being burdened by changes that are too prescriptive. At the same time we will need to consider any impact this will have on other rights of individuals, including freedom of expression. I would like to think these views are shared by many of you here today.

- The UK's approach to legislative change in this area is something that I and my colleagues will return to. What I can say now is that it is likely to be informed by a number of factors, including:
  - o A proper evidence-base for the proposed legislative change;
  - o The actual benefits to data subjects;
  - o The resource implications for data controllers;
  - o The impact on, and views of, our Information Commissioner as well as other experts in the field of data protection;
  - o The needs to cater for the specific needs of law enforcement bodies due to the distinctive nature of law enforcement work
  
- In the UK, we have, and will continue to, engage extensively with relevant stakeholders, within government and outside it. Key private sector stakeholders include IT and online firms, credit reference agencies and telecommunications companies as well as those bodies concerned with the protection of personal data and privacy. In this way, we want to have clear evidence and examples to support our position so that the legislation can be flexible and take into account modern and emerging technologies.
  
- Let me finish by returning to Convention 108. The UK strongly advocates and would encourage support for the example set by the Council of Europe's work in modernising Convention 108. Indeed, it is my contention that the Council of Europe's emphasis on guiding principles, proportionality and flexibility should serve as the foundation for the European Commission's work on updating its own data protection regime. If it is the case that we have before us two contrasting approaches to the future of data protection, two possible visions of where we might end up, I believe it is the Council of Europe's approach that has shown itself to be the more viable - for it is proportionate, workable and sensible. And, it's on that note that I would like to underline my support for the continuing work of the Council of Europe and representatives from member states in modernising this ground-breaking instrument which has set a world wide standard in the field of data protection. I trust that by working together we

can secure protections for the public without sacrificing the vital freedoms on which we all depend.