Spring Conference Keynote

Christopher Graham

… The theme of this year’s conference is highly relevant. Navigating the digital future: Let’s get practical.

The activities we regulate – the collection, processing, and security of personal information – and the rights and responsibilities we exist to uphold – privacy, integrity, and personal autonomy – are changed and challenged by the digital revolution. That means that Data Protection Authorities like ours, whether or not they are in the European Union, are challenged too – to respond to the realities of what digital means, and to be able to continue to uphold the fundamental rights for which we stand. And that means change for us too – if we are to be effective at what we were set up to do.

We meet 30 years after the coming into force of the Council of Europe’s Convention 108 – and 20 years after the European Community’s Directive 95/46. To say that much has changed over the decades is to state the obvious.

And much has changed even in the six years since this European data protection family last convened in the United Kingdom – at the Edinburgh Spring Conference in 2009. But some things don’t change, or don’t change at the pace of everything else that is happening.

In Edinburgh, the talk was of data protection reform in Europe. A report from the Rand consultancy proposed a new approach to regulation. But we had to wait a further three years almost for proposals from the European Commission for a reform of the 1995 Directive. And, as we all know, three years later still, we are still waiting for Member States to come to a common position, allowing the Trilogue between the Council, the Parliament, and the Commission to begin. Even after agreement on the final text of the proposed Regulation, it will be another couple of years before the new rules are in force.

Has the digital revolution paused while the European Union decides what to do? I don’t think so.

The concerns that first animated the Council of Europe more than 30 years ago were fears of the misuse of personal information stored in vast databases on huge mainframe computers. The fear was of the misuse of computers by governments and big corporations. And that seemed to be the issue 30 years ago. After all, 1984, was the title of George Orwell’s classic story of Big Brother, the Thought Police, and the Ministry of Truth.

But that was before the advent of the mobile phone and texts, the Internet and email, satellite television and digital radio, globalisation, the end of the Cold War and the start of the first Iraq War.

Today the digital revolution has implications for every aspect of our lives – as citizens, as consumers, as individuals. We communicate. We consume. We transact. And, unless we are very alert, we are also tracked. Shopping in the supermarket or online, our purchasing habits are recorded and analysed. We live in a world of Big Data and the Internet of Things.

Governments too have gone digital, keen to find efficiencies in the delivery of joined up public services. And now there’s the security dimension, with politicians claiming that public safety is an absolute right, while privacy is a right that may need to be qualified.

We know all that and we are working hard doing what we do, you might say. Why do data protection authorities need to change? Surely we just need to hold to fundamental rights even more in the new and changing circumstances. After all, privacy has never been more important – or more threatened.

And that’s where we need to get practical. Because the challenges are to how we do things, not what we are there for. If we want to be effective doing what we do, we are going to have to learn to do some things differently.

The best place to begin is by understanding what is expected of us – by the people whose fundamental rights we are supposed to be defending.

The research paper circulated in preparation for this conference is a start. What the public want in terms of data protection and what the public want from Data Protection Authorities. We’ve pulled together the findings of recent Europe-wide research by such respected organisations as Eurobarometer and the Fundamental Rights Agency (FRA). We’ve included the findings of UK organisations such as Citizens’ Advice. And, specially for this conference, we commissioned some focus group work involving UK consumers and citizens who regularly use the Internet. Last month, BDRC conducted focus groups with ‘less knowledgeable users’, those with ‘some knowledge’, and others who claimed to know a lot. It turns out that British data subjects conform to the pattern identified in the Europe-wide research.

Across all the studies, the commonly recurring themes of what the public want from data protection are;

• Control over their personal data;

• Transparency – they want to know what organisations will do with their personal data;

• To understand the different purposes and benefits of data sharing;

• Security of their personal data; and

• Specific rights of access, deletion and portable personal data.

The themes of what the public want from DPAs are;

• Independence – DPAs free from outside influence;

• Consistency – where possible a consistent approach to data protection across the EU;

• Visibility – DPAs making themselves known, providing clear help and guidance to them and also to organisations;

• Privacy certification, seals and trust marks – giving them confidence in the organisations who are processing their personal data;

• Responsive to new technologies – DPAs that understand the privacy implications of the new technologies they encounter in their daily lives; and

• Enforcement – appropriate remedies that are used effectively by DPAs to ensure that organisations comply with data protection rules.

Those of you who have already studied the paper will have seen quoted frequent examples of how the ICO does things. It is important to understand that they are only examples. I’m proud of what the ICO is doing, but in saying that I’m not claiming that the ICO way of doing things is necessarily the best – still less that everyone has to do things the British way. In fact, the research itself has some hard lessons for the ICO too.

We like to think we are fairly high profile, but our annual track of public attitudes told us that only 1% of those questioned would think of going to the ICO for advice on their rights to protect their personal data. This despite 97% prompted awareness of data protection.

The point is that citizens and consumers attitudes to privacy are changing as they become accustomed to the digital deal. What’s in it for me, if you like. Public attitudes and awareness may not be uniform. Tech savvy youngsters may not have thought through the implications of being quite so free with their data. Older people may not always understand quite what’s going on (although I like to quote my former mother-in-law as an example of a so-called Silver Surfer who was very much alert to the realities of digital. Techno Gran, we called her.) But we have to understand what today’s data subjects understand about data – and what they expect of us as the guardians of their fundamental rights.

If we just carry on doing what we do, the way we’ve always done it, regardless of what’s been happening over the last 20 or 30 years (and what might happen over the next few decades), oblivious to what consumers and citizens are doing for themselves, and ignoring what they are telling us about what they expect from us data protection authorities, we won’t be doing our job as regulators of data, guardians of privacy and policemen of the digital highway.

The trouble is that knowledge of data protection has the potential to be arcane and obscure. We, the initiates, can delight in the certainties and peculiarities of, for example, the 1995 Directive. But to do so, without being open to new developments, risks turning ourselves into the devotees of some mysterious religion, debating how many angels can dance on the head of a pin, professors at the University of Data Protection, more interested in theory than practice.

I’m sure it’s apocryphal, but you know the story of the expert who was asked what he thought of some new development in his field. It’s fine in practice, but does it work in theory?

Of course, for those of us in the European Union, it’s difficult to know quite how we should be changing when we don’t yet know exactly what will be required of us under the data protection Regulation, not to mention any Directive on police and justice matters. But some things are clear – in outline, if not in detail. The European Data Protection Board, for example, is coming - and it is going to be a reality within the next two or three years. That means we in the Article 29 Working Party family have to learn to co-operate and work together better. An ever closer union, if you like.

And co-operation between European agencies is firmly on the agenda following last year’s conference in Strasbourg. Not just co-operation within the EU, but co-operation between data protection agencies within the Council of Europe framework. We’ll be hearing more about this tomorrow and we have a resolution on the same topic.

But we are not dealing with purely European phenomena. Co-operation within Europe is certainly necessary, but it’s not sufficient. The threats to privacy are global in nature and they require global responses. A year ago the ICO welcomed many of you to Quarry Bank Mill near Wilmslow for the annual international enforcement co-ordination meeting under the authority of the International Conference. Next month, some of us will be in Ottawa, building on the progress made at Mauritius on the Global Cross Border Privacy Enforcement Arrangement. And of course we are looking forward to the Amsterdam conference in the autumn – with its theme of building bridges between different approaches to data protection and privacy.

So we need to be better joined up and work better together in the face of global developments and multi-national players. This doesn’t just mean individual authorities working better together, but closer working between networks of authorities too.

By pooling our efforts, we not only address more effectively the challenges that come from outside our individual jurisdictions, but we also make better use of the limited resources of money and people we have at our disposal. More on that later.

And working with others is not just about co-operation between DPAs. We have to find ways of being heard and being effective by partnering others who are travelling with us along the privacy road. These might be national sector regulators with whom we can co-operate. But also, perhaps, industry trade bodies or self-regulatory organisations with an interest in raising standards of compliance. The draft Regulation, at Article 39, speaks of certification mechanisms and data protection seals. On pages 31 and 32 of the research paper you can read about the Privacy Seal programme the ICO is developing.

In the face of the scale of challenge we face, we will only be effective if we accept that we will not achieve anything worthwhile if we try to do everything, including some activities that are worth very little in any event. ‘Less’ really is ‘more’ – or as my predecessor Richard Thomas used to put it ‘Be selective, to be effective’.

Certainly, the obligations to be met by data controllers must be clear. But it does not make any sense to prescribe in minutest detail the procedures to be followed by every data protection authority in order to secure compliance.

Three years ago, I was assured by Peter Hustinx no less that the obligation laid on DPAs always to fine data controllers in the event of any of a list of failures would be changed to an enabling mechanism. Not ‘shall fine’, but ‘shall be empowered to fine’.

It would be a mistake to believe that data protection authorities will be issuing huge fines left right and centre. Fines can only follow investigation and often involve appeals. We have to follow due process which requires resources. ICO experience is relevant here. In 2013, we imposed a £250,000 penalty on Sony Computer Entertainment Europe Limited after finding the company had not taken sufficient steps to prevent the loss of "vast" amounts of personal data belonging to millions of UK consumers. How, under any new framework, would we work out what the Global turnover of Sony is – and they’re much more likely to fight us over 2% or 5% of that figure than the £250,000 fine we imposed.

The availability of fines of up to 2% of global turnover (or 5% in the Parliament’s text) is important. It makes the punishment fit the crime – and fit the perpetrator. But DPAs need the discretion to be able to focus on the biggest threats, not be forced to fine every case of non-compliance regardless of priorities. Again, selective to be effective. And effective it would be, because data controllers would know that it could be them.

That is the experience we have seen in the UK following the introduction of a civil monetary penalty power. Since 2010, the ICO has been able to impose fines of up to £500,000. We’ve imposed 68 such fines, totalling just over £7.5 million. But our research (page 36 of the paper) shows that the fact that the ICO can impose fines has had as big an impact on businesses we haven’t actually hit as it has on the businesses who have had to pay. In other words, like General De Gaulle and deterrence theory, the power of the deterrent lies in the uncertainty around whether or not it will actually be used. And it’s cheaper too.

This brings me to the very practical - paying for everything DPAs are supposed to do. I am very conscious that, with more than 400 staff and a budget of around £17 million for data protection alone (we also have responsibility for Freedom of Information), the ICO is one of the bigger and better resourced of the European DPAs. But, whatever the scale of their operations, individual data protection authorities must be assured of the funding necessary to do what is expected of them. Again, we’ll debate this tomorrow – and, I accept, it is for Member States to secure the funding of their national DPAs.

And here it is worth challenging the politicians. Don’t legislate for what you are not prepared to fund. It’s said one should never confuse a memo with reality. In other words, just writing something down doesn’t change anything.

It’s not job done. It’s job hardly begun.

Similarly, a mere Regulation has no value in itself. It’s just words - and more words. The years spent drafting, debating and amending a text will only have been worthwhile when it starts to be applied – and when DPAs have the resources to take on the priority offenders without being bogged down with costly, but low-value routine obligations and processes.

And that is where the Commission’s role will be key. Having proposed the reform, the Commission will itself need to compromise in order to secure a final text that is practicable. Yes, the Member States have to fund their DPAs, but the Commission, and the Parliament too, must not insist in the Trilogue on processes that can only render small, under-funded DPAs ineffective – or less effective than they could be if given space to prioritise their interventions. It’s only job done if it’s job doable.

So, let’s get practical – all of us. The programme over the next two days suggests ways of doing just that.