Information Commissioner's Office

National Police Chiefs' Council Information Practitioner event

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/06/npcc-information-practitioner-event/

Date: 07 June 2017
Type: Speech

Original script may differ from delivered version

Elizabeth Denham talks data protection and policing at the NPCC Information Practitioner event, in Kenilworth, Warwickshire.

Good morning, and thanks for inviting me to speak at today's event.

I know, after the terrible attack in London on Saturday, and a fortnight ago in Manchester, that this has been a testing month for you. And I know for some of you who experienced the impact of these attacks first hand it will have been particularly challenging. We should need little reminder of the important role the police provide, but last month's events bring into sharp focus the bravery and professionalism of the blue light services.

I have been invited here to provide a regulator's view of what lies ahead, building on the practical advice around data breaches that many of you will have enjoyed at yesterday's workshop by my colleagues in our enforcement team. As I said in the foreword of your event programme, it is clear this is a crucial time for information rights in this sector. I've been here for almost a year, and getting a feel for policing in the UK, what the reality is on the ground, has been a priority for me. It's clear from the initial meetings I've had with senior leaders like Ian Dyson, and Cressida Dick, and Ian Readhead that the speed of technological change, and more integrated information systems offer ways to have a real impact on frontline policing.

But there are pressures too. The ICO received more than 18,000 data protection complaints from members of the public last year. One in twenty concerned policing and criminal records. A similar proportion of our self-reported data breaches s concern your sector. And you'll have seen and heard about the penalty issued to Greater Manchester Police earlier this year.

But I am not here to examine where our office has had to investigate or enforce the law in this sector I am here to underline public safety and individual rights are not in competition – public trust in policing requires respect in how you handle personal data.

The General Data Protection Regulation (GDPR)

Let's start with the law. No-one in this room will be surprised to hear me say there is still uncertainty around data protection legislation in this sector.

So what do we know? The GDPR will happen. On May 25 2018, the new law will be implemented. While it builds on the previous legislation, make no mistake that it is the biggest change to data protection law in a generation. It brings a 21st century approach to the processing of personal data, providing much more protection for individuals, and more privacy obligations for organisations.

Our website provides an overview for those of you wanting to get across the specific changes, and our self-assessment toolkit has a checklist to help you prepare for GDPR. It's also important to be aware of the obligations for organisations to report data breaches that pose a risk to individuals to us at the ICO, and in some cases to the individuals affected.

Law Enforcement Directive

But as you will be aware, things are a little more complex around policing. The GDPR does cover personnel records, and any non- policing activity, but it does not cover the use of personal data for law enforcement purposes. Unlike the DPA, it does not cover a lot of your work. Instead – as you'll have heard from DCMS if you were here yesterday - there is a separate legal instrument, the Law Enforcement Directive. This covers the use of data for law enforcement purposes, but, in simple terms, in the UK its scope could be limited to data processed for certain European Justice and Home Affairs measures.

The Directive does not automatically become UK law: the government must implement it in the UK. And so far the government has not made any public announcement in terms of detail on how and when that might happen, and what their position is around data processing for domestic law enforcement. We've spoken to the Home Office and DCMS and expressed our concern about how late in the day this is being left. I'm certainly sympathetic to forces needing time to prepare for any law changes. And there's a bigger picture here too. Maintaining appropriate data flows is essential for law enforcement and security purposes. I know from speaking to senior figures in the sector that, for anti-terrorism, for security and for justice, you need to maintain access to databases – to Europol, to Eurojust, and to the Schengen Information System. This needs to be a very high priority for the next government in the exit negotiations.

Opportunity

It is clear there is uncertainty here. I would like to give you more definitive answers, but that is not in my gift: we simply have to trust that the government will resolve this by next May. But it's important to realise there's opportunity here too.

Firstly, there is an opportunity to prepare for what is coming. While the legislation is not clear, the direction of travel is. A cursory look over any data protection reform around the world brings up the same key threads running through: more requirements to log what you're doing with data. Mandatory breach reporting. And data protection officers who are accountable to senior management.

These are all central parts of the GDPR, and it's difficult to imagine they won't form some part of the requirements government will set out for UK police forces.

And then there's accountability. This is perhaps the most notable change between the current Data Protection Act and the GDPR. The new legislation creates an onus on organisations to understand the risks that they create for others, and to mitigate those risks. It's a demand that senior leadership move away from seeing the law as a compliance exercise and instead build a culture reflecting the value of properly caring for data.

That value exists for police forces as much as for other organisations. Data protection is changing. People expect more of organisations: they're more aware of their rights, they expect their information to be looked after properly, and they expect it to only be used in ways the law allows. Organisations, including police forces, need to respond to that, and these changes give them an opportunity to take a look at how they're doing things. Accountability is a legal trend that we've seen in other parts of the world, and will surely have some part to play in domestic legislation.

The Police National Computer (PNC), Body Worn Video (BWV) and Automated Number Plate Recognition (ANPR)

Irrespective of the law changes, there is no time for anyone in this room to sit on their hands for twelve months. There is still plenty to be looked at today, under the current Data Protection Act. There are plenty of questions I feel police forces are still struggling to answer.

Let's start with the retention of PNC records. Why are records being kept so long? It's a full year since my predecessor Christopher Graham was asking in a foreword to this event how it could be proportionate for an arrest record to be held on PNC until an individual reaches 100 years of age.

My view is no different. The law requires proportionality. That gives plenty of room for police forces to hold some data longer than, say Tesco hold your Clubcard info. But that does not mean that you can ignore data retention principles.

The same is true of the technologies that form a growing part of modern policing. How are people's legal data privacy rights being protected? Data protection law should not unduly prevent the police from detecting, investigating and deterring crime, but it does demand proportionality.

There are similar questions to ask around techniques that collect large and indiscriminate amounts of personal data. I've spoken to police officers and security specialists. I understand the benefits that come from new and better use of ANPR, from drone technology and body worn cameras. But detecting crime does not mean a free pass.

Freedom of information

It's a similar picture around the freedom of information law. The important role that police forces play in society does not exempt you from responding when the public asks for information – in fact quite the opposite.

I know forces are getting more requests, and I know budgets – and in turn the number of people you can call on to help answer requests – are being squeezed. But the public expects that their rights are respected. I'm upping the threshold for what we consider to be an acceptable level of service. I expect public bodies to respond to 90% of requests within the statutory time limits, or you run the risk of falling foul of our monitoring regime.

Why is that? Those statutory timeframes are statutory for a reason. Freedom of information is important. I'd consider it is a part of our modern constitutional settlement, and a crucial tool for public scrutiny.

I should add that there is more to this than simply handing over records when asked. The duty to document should be a fundamental part of this picture, and accurate police records are necessary to protect citizens' rights and inform policy and historic study. I will be studying the evidence –across the public sector - to become fully informed of the scale of challenge of ensuring that important records of decisions made are created and retained. Staff in my office will conduct policy work in the coming year to help us obtain a deeper understanding in this area, and I won't be shy in advocating for a legislated duty to document if I think it is required.

Proactive transparency is also important here. I know some forces want to do more in this area, and I can see why. Proactively disclosing information – showing accountability and transparency by publishing important information before people ask for it – has obvious advantages. In my mind it would never replace the freedom of information right to request information, but it could go some way to further building up the trust you have from the communities you police.

Social licence

Some of you in this room may take quite a binary view of what I'm saying today. If the law allows us to do something, you might think, then we'll do it. If the law doesn't allow us, then come and knock on our door. It's black and white. But that isn't the reality. Police forces operate under a social licence. They require the trust and faith of the societies they police. We only have to look to parts of the USA to see the problems that can ensue when that public trust and faith starts to erode.

And data protection – how forces look after data, the respect they show for the information they're provided by witnesses and victims, the volume of information they're recording and the length of time they're keeping that information – that all plays in to the trust people have in you.

Over the past few years ICO casework has shown that UK citizens are better informed around their information rights than ever before. But I think it's also clear that a lot people feel they've lost control of their own data, that their sense of power over their personal data has slipped its moorings.

That sense of loss of control impacts their trust in organisations. A police force isn't like a business – it's not as simple as to say people will take their custom elsewhere. But failing to recognise that having access to people's personal information means you have to act with great responsibility will have consequences.

As I spoke about earlier, the government will need to step in to set out data protection law for law enforcement. Any government doing that would surely take on board the views of the electorate.

The Information Commissioner's Office

But let’s not end on a negative. As I said earlier, there is an opportunity here. And my office will be here to help along the way. We’re working hard to provide the advice you need around GDPR, and we’ll do the same as and when we have a clearer picture of any new law.

Keep looking at our website. Keep an eye on our enewsletter, our twitter, however it is you keep up to date with the work we’re doing. And if you’ve got any questions for us, then get in touch. Use our helpline. Use our live text.

We live in interesting times. And particularly within this room, we live in uncertain times. But while the exact form of the legislation may vary the route, the direction of travel for privacy and data rights is still the same. I hope we can help you get there as quickly and easily as possible.

Thank you.