ico.
Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.gov.uk

343908

Ministry of Justice

29 MAY 2013

Received

Rt Hon Chris Grayling MP
Secretary of State
Ministry of Justice
102 Petty France
London
SW1H 9AJ

24 May 2013

Dear Secretary of State

**DRAFT EU GENERAL DATA PROTECTION REGULATION**

When we met earlier this month I expressed my concern about the ability of my office to make the proposed EU general data protection regulation work in practice. I said I would write to you before the Justice Council next month to expand on my concerns.

My worries were set out in the evidence that I and my Deputy David Smith gave before the House of Commons Justice Committee on 4 September 2012. The ICO believes that the right legislative approach can still result from negotiations involving the Council and the Parliament. We certainly see the need for a data protection regime that is more attuned to the requirements of the 21st century. In particular, in the European Commission's proposal, we welcome

- Improved rights for individuals, including consent
- Clear responsibilities on data processors
- Introduction of accountability for data controllers
- Recognition of the need for data protection by design and data protection impact assessments
- Stronger supervision and sanctions

My duty as UK Information Commissioner, however, is to draw attention to the burdens that the Regulation, as currently drafted, would place on my office and other data protection authorities (DPAs), and the impact that this would have on our ability to uphold information rights in practice.

As things currently stand, for all the recent talk about proportionality and risk, I see real problems ahead with the practical delivery of a Regulation that is still so detailed and specific as to the processes DPAs shall undertake in almost all circumstances. Of particular concern are

- The emphasis on punishment and sanctions at the expense of awareness raising and education
- The requirement for all data breaches to be notified to the DPA, rather than just those that pose significant risk
- Prior authorisation to be required for all international transfers where this is not required under current regime
- Limited discretion for DPAs over administrative sanctions which are imposed on the basis of process failures rather than privacy risks
- Participation in a consistency mechanism that is insufficiently risk based and contains unrealistic time-limits

Such a regime is bound to be very costly, and my concern is heightened by the fact that it is by no means clear where the money is going to come from to fund it. The Commission's long-promised study of the funding of DPAs has still not been published; but, given the state of the public finances across the EU and the more obviously higher priority causes competing for funding, it is surely questionable that there will be much more money available for DPAs than there is now. Yet more spending by DPAs is what the Regulation assumes.

In the case of the UK, the problem is compounded by the fact the abolition of the notification system calls into question the ICO's current source of funding. The ICO's data protection work is funded by notification fees. In the last financial year this income amounted to £16 million. We do not yet know how this funding is going to be replaced or how alternative sources of income would avoid compromising the ICO's necessary 'complete independence'.

The 'consistency mechanism' proposed in the Regulation must involve net additional expenditure as DPAs have to support and co-operate with the DPA in the country of main establishment, although there may be some modest efficiencies from the different DPAs not having to duplicate full investigations of similar cases within their own jurisdictions. But the system will only be as good as its weakest link.

Information Commissioner's Office

It would be most unfortunate if any lack of funding led to forum shopping with data controllers targeting the smaller and less resourced jurisdictions or, by contrast, moving their operations in order to deal with those DPAs who were best placed to process their business. In the case of the ICO, we can anticipate a good deal of 'country of main establishment' business simply because the UK is one of the larger economies in the EU, and that would require further resources still.

Without significant additional resources it is clear that the ICO would need to change its regulatory approach. Instead of giving advice and guidance and intervening on the basis of risk and proportionality, we would have to move towards a process-driven approach based on prior checking, processing of breach notifications, and mandatory fines. To the extent that we could no longer be selective on the basis of a regulatory risk-based judgment, I fear we would be less effective. If this is true for the ICO, one of the biggest and best resourced DPAs in the EU, questions have to be asked about the viability of the proposed Regulation elsewhere in the EU.

I very much hope that a way can be found to finalise a data protection regime that is fit for purpose - modern and effective, and delivering for citizens, consumers, and the enterprise economy.

While these representations are totally consistent with what the ICO has been saying throughout the reform process, in view of the widespread interest in these matters I propose to post this letter on the ICO website in the week beginning 3 June.

Yours sincerely

Christopher Graham

Christopher Graham
Information Commissioner

Telephone: 01625 545709
Email: Christopher.Graham@ico.org.uk