Data protection reform

Latest views from the ICO

The ICO is publishing its further thoughts on the reform of Europe's data protection rules in light of recent announcements from the European Parliament, Council of the European Union and European Commission.

- This is a **great opportunity** to update data protection law to reflect the way personal information is used today and will be used in the future. **We need more effective rights for individuals** – including greater control over their personal information - and **clearer responsibilities** for those that process information about them. However, we have to get it right now – both with the General Data Protection Regulation and the Directive relating to criminal law enforcement and judicial activities - as the next generation of data protection law will be in place for many years to come.

- However the law is implemented in Member States, there needs to be **as much consistency as possible** between the various instruments. Any substantive inconsistency between a General Data Protection Regulation and a criminal / judicial processing Directive will be a source of **difficulty and confusion** for years to come. For this reason, any move to create a separate instrument governing processing in the public sector should be resisted.

- The current proposal is **too prescriptive** in terms of its administrative detail and the processes organisations will have to undertake to demonstrate accountability. This could be a particular problem for SMEs. The European Parliamentary efforts seen so far are on the right track but could be more ambitious: there needs to be more emphasis on **outcomes rather than processes** and for a truly **risk-based approach** to compliance.

- The **scope of the law** needs to be as clear as we can make it, particularly the definition of '**personal data**'. In particular, the status of pseudonymised data needs to be clarified and, if covered, needs to be treated realistically for the digital information society age. The same considerations apply to **non-obvious identifiers** such as logs of IP addresses generated online. This is important in areas as diverse as medical research and internet content delivery.

- Individuals need **dependable rights**. This means rights they understand and that can be delivered in practice. Individuals need more control over their personal information but there is a danger that the '**right to be forgotten**' will lead them

to expect a degree of protection that cannot be delivered in practice. We also need to be realistic about the limited power EU data protection authorities may have over **non-EU data controllers**.

- Different Member States have **different legal traditions**. What is allowed by law is not spelled out in the UK in the way that it is in some other countries' legal systems. The proposed legislation needs to reflect this, particularly in relation to the concept of '**legitimate interests**'.

- We support a **high level of consent**, so that there is as little doubt as possible as to whether individuals have - or have not - agreed to their personal data being processed in a particular way. However, there must be a coherent set of **alternatives to consent** for situations where consent is not viable.

- Citizens across the EU should have broadly **the same information rights**, and data controllers **broadly the same responsibilities**. However, this does not mean every detail of the law has to be harmonised. For data protection law to make sense there has to be scope for flexibility and recognition of genuine and fundamental differences in national legal traditions.

- European data protection law also needs to be **outward-looking**, to open the way for greater interoperability beyond the borders of the EU. Greater emphasis on the principles of data protection and on outcomes, and less on the administrative detail, particularly in relation to the approval of international data transfers, will facilitate this.

- **Data protection authorities** will need **adequate resources** to carry out the many new functions they may be tasked with, and to maintain their independence. A more risk-based approach in the law would allow data protection authorities to maximise their effectiveness by **focussing on high-risk data processing**. This will become even more important in the future given the constant and rapid expansion of data processing activity across the EU and beyond.

- The Parliament has sensibly proposed to leave it to the European Data Protection Board to ensure **consistency in relation to sanctions**. The ICO notes the impracticality of linking the sanction to percentage of turnover. Fines are not always the solution. Data protection authorities should work together towards a genuinely risk based approach, with more discretion over the use of sanctions.

- Further clarity is needed on how the proposed Directive will apply in the UK. We must ensure that data protection rules whether about processing personal data domestically or for cross border purposes are **as consistent as possible**. There must be **a clear understanding of how the law applies** to personal data processed in these law enforcement contexts.