The EU data protection reform proposals continue to generate much discussion. The UK Information Commissioner agrees that the current European data protection regime needs to be updated, as the ways in which personal data is collected, held and processed have changed significantly since the Data Protection Act 1998 came into force. The Commissioner sees the proposed new EU General Data Protection Regulation, (the “Regulation”) as a chance to modernise data protection law. However, the Commissioner – amongst others – has also expressed some concerns about how certain aspects of the proposed new Regulation will work in practical terms.

In recent months, the Commissioner has expressed his views on many aspects of the proposed Regulation including the much debated suggestion of additional flexibility for the public sector, pseudonymisation, governance, international data transfers and the adoption of a risk based approach to data protection – which the Commissioner is firmly in favour of. In a recent letter to the Ministry of Justice, the Commissioner highlighted various proposals within the new Regulation that he approves of. For example, the proposed new clear responsibilities for data processors and increased accountability for data controllers as well as the improved rights for data subjects, including consent.

The draft Regulation defines “the data subject’s consent” to mean “any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed”. The Regulation also includes a number of conditions for consent. The requirement for consent to be explicit is still being debated but the Commissioner welcomes this high standard of consent while noting that alternatives to consent are also necessary. However, the letter also sets out a number of areas of concern.

The ICO is also generally in favour of the proposals regarding data protection by design and data protection impact assessments. Broadly, the proposals would oblige data controllers to implement appropriate technical and organisational measures and procedures to make sure that their processing activities meet the Regulation's requirements and ensure protection for data subjects’ rights. Controllers would also have to implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are not collected or retained beyond the minimum necessary for those purposes. The proposals also broadly require data controllers – or processors acting on their behalf – to carry out an assessment of the impact of their proposed processing operations on the protection of personal data in circumstances where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, scope or purposes.

The Commissioner also welcomes the stronger supervision and sanctions proposed by the new Regulation. Among other things, the Regulation proposes administrative sanctions, which allow supervisory authorities to impose larger fines for more serious breaches with the most serious breaches attracting fines of up to 1,000,000 EUR or, in the case of an
enterprise, up to 2% of its annual worldwide turnover. The Commissioner broadly approves of these proposals, although would prefer a more flexible approach based on a non-ranked list of breaches with the actual effects of the breach being taken into account to determine the applicable penalty.

Among the areas of concern, which were highlighted in the Commissioner’s letter, were the emphasis on punishment and sanctions at the expense of awareness raising and education; limited discretion for data protection authorities over administrative sanctions which are imposed on the basis of process failures rather than privacy risks; and participation in a consistency mechanism that is insufficiently risk based and contains unrealistic time limits.

The Commissioner is also concerned by the requirement for all data breaches to be notified to the data protection authority, rather than just those that pose significant risk. The Commissioner feels that some breaches will be more significant than others and potentially the ICO will have to address a very large number of data breach notifications, some of which may be relatively insignificant. The Commissioner is also worried that data controllers would be obliged, without undue delay and, where feasible, not later than 24 hours after having become aware of it, to notify all personal data breaches to the supervisory authority, believing these timescales to be unrealistic and also potentially inconsistent with the Privacy Directive 2002/58/EC.

The Irish Presidency of the Council of the European Union has recently prepared a draft compromise text on the Regulation which has suggested, (among many other things), an extension to the timescales to 72 hours and suggests that only breaches which are likely to severely affect the rights and freedoms of data subjects need to be notified to the supervisory authority and the relevant data subjects. This may help alleviate the Commissioner’s concerns somewhat.

Another issue for the Commissioner is international data transfer. The new Regulation envisages greater involvement for data protection authorities in approving arrangements for protecting personal data being transferred internationally and prior authorisation of international transfers and methods by which such transfers are made in many circumstances. These requirements are very different to the current approach in the UK and the Commissioner is concerned that introducing prior authorisations for transfers will be a burden on the ICO.

The Commissioner has also highlighted the potential cost of implementing certain aspects of the new regime and the sources of funding which will be available to finance it; noting that abolishing the notification system will undermine the ICO’s current source of funding and that lack of funding could lead to forum shopping. It has been highlighted that without further funding the ICO would have to alter its regulatory approach, becoming process-driven and basing its approach on prior checking, processing of breach notifications and mandatory fines, which could make it less effective.

Many of these issues are still subject to further discussion. The draft Regulation is likely to be subject to considerable and further debate before a final text is agreed. It will be interesting to see whether the contentious issues are resolved to the Commissioner’s satisfaction.

The original version of this article can be found here:

For more information about this update, please contact Clare Sellars, Partner, on 0207 822 1969 or clare.sellars@weightmans.com

This update does not attempt to provide a full analysis of those matters with which it deals and is provided for general information purposes only and is not intended to constitute legal advice and should not be treated as a substitute for legal advice. Weightmans accepts no responsibility for any loss that may arise from reliance on the information in this update. The copyright in this update is owned by Weightmans LLP 2013.