The Citizens' Rights Directive
On 18 December 2009, the Citizens' Rights Directive 2009/136/EC (the "**Directive**"), which amends, among others, the e-privacy Directive 2002/58/EC, was published in the official journal.

The Directive introduces three main changes to the legislation, which are likely to have wide implications for consumers and businesses. In particular, the Directive establishes a notification regime in case of data security breaches, a new regime for cookies and widens the scope of the rules on unsolicited electronic marketing, i.e.: the anti-spam rules.

The Notification Regime
The notification regime applies to providers of publicly available electronic communications services, i.e.: providers of: (i) fixed and mobile services; and (ii) e-mail networks and internet services. The regime does not apply to providers of online services offering other information society services. This means that the notification regime should apply to telecom providers and ISPs, but not to online retailers, banks and the like.

The Directive requires providers of publicly available electronic communications services to notify the national data protection authority, without undue delay, any personal data breach. This includes any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the EU.

The Directive provides also that when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay. Note that the decision to notify subscribers or individuals is up to the provider, although, in case of the provider's failure to notify, the national data protection authority may require the provider to do so.

The provider's duty to notify subscribers or users does not apply if the provider has demonstrated that it has implemented appropriate technological protection measures, which the competent data protection authorities may audit. The notification to subscribers or individuals should describe the nature of the personal data breach, the contact points where information can be obtained and shall recommend measures to mitigate the possible adverse effects of the breach. Finally, providers are required to maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken.

The introduction of the notification regime represents a major change for providers of publicly available electronic communications services, which will have to adopt procedures to ensure that they comply with their notification duty without impacting too much on their business. This will probably require the adoption of streamlined procedures and the appointment or identification of personnel responsible for the notification requirement.

Cookies
The Directive addresses cookies and other forms of tracking technology by providing that such devices may be placed on subscribers' and users' computers only where subscribers and users have given their consent, having been provided with clear and comprehensive information about the purposes of the use of such devices. Note that there are exceptions to the consent rule as cookies and other tracking technologies are permitted where they are necessary for the sole purpose of carrying out the transmission of a communication over an electronic communication network or where they are strictly necessary for the provision of a service explicitly requested by the user. Additionally, Recital 66 to the Directive provides that users' consent may be expressed by using the appropriate settings of a browser or other application. Note that the rules on cookies apply to anyone using cookies or other form of tracking technology.

The provisions on cookies, if strictly implemented, are likely to hinder the ability of website publishers to raise revenue through online advertising as they will be required to seek users' consent via the use of "pop-ups" or other similar devices. Regrettably, these are likely to render surfing the web an unpleasant experience for many users. Additionally, it is not clear how the exceptions to the consent rule can be relied on, especially the one contained in Recital 66. At the conference on personal data online the Information Commissioner's Office ("**ICO**") was unable to comment on the UK implementation on the Directive's rules on cookies. Accordingly, it is difficult to predict whether this will be pragmatic or prescriptive.

Unsolicited Marketing Communications

The rules on opt-in and soft opt-in in relation to unsolicited electronic marketing communications are widened in the Directive, as they cover users and not only subscribers. 'Users' has a wider meaning than 'subscribers', as 'users' covers any individual using the communications systems and not only those individuals, who pay for the systems.

Additionally, as the Directive requires consent in relation to unsolicited marketing communications sent via communications systems, it may be possible that this will impact on Bluetooth marketing. Bluetooth marketing is currently exempted from the consent rule as it does not travel on a subscribed network. However, as 'communication systems' is currently not defined in the Directive, it could be that a future interpretation of it may include Bluetooth, thus bringing Bluetooth marketing within the reach of the consent rule when it is forced on users.

Finally, the Directive gives legal persons with a legitimate interest in combating the sending of unsolicited commercial emails the right to take legal action against spammers in civil proceedings.

The UK has until 26 April 2011 to implement the Directive. If this is transposed faithfully, there will be wide repercussions on businesses and consumers and possibly little scope for the ICO to take a pragmatic approach.

New Notification Fees

Further to the consultation exercise by the Ministry of Justice ("**MoJ**") in summer 2008, a new notification structure has been introduced since 1 October 2009. The new structure is based on a two-tiered fee and applies to notifications and annual renewals of register entries. The criteria to establish whether a data controller is in Tier 1 or Tier 2 is based on whether they have a turnover of £25.9 million or more and whether they have 250 or more members of staff, except where the data controller is a public authority. Public authorities with 250 or more staff will fall into Tier 2.

Accordingly, where the data controller has fewer than 250 members of staff, the data controller is in Tier 1 and the fee payable is £35. Where the data controller has 250 members of staff or more and a turnover in the last financial year of £25.9 million or more, then the data controller is in Tier 2 and the fee payable for notification is £500.

Note that 'members of staff' means any employees, workers, office holders or partners. With regard to companies belonging to a group of companies, each company within the group is required to assess the members of staff and turnover with regard to itself and, not in relation to the overall group figures.

The ICO New Penalty Powers

On 9 November 2009, the MoJ launched a consultation proposing that the ICO be given the power to impose civil monetary penalties of up to £500,000. The MoJ's consultation ended on 21 December 2009. On 12 January 2010, the MoJ published the summary of responses to the consultation. This states that of the 52 responses, 27 supported the proposal that civil monetary penalties of up to £500,000 provide the ICO with a proportionate sanction for serious contraventions of the data protection principles. Accordingly, this new system of penalties is very likely to come into force on 6 April 2010, depending on Parliament's approval.

While the new penalties will apply to all data controllers, including government departments, private sector companies and charities, they will not apply to individuals processing personal information for the purposes of that individual's personal, family or household affairs as this is exempt under the Data Protection Act 1998.

The ICO will publish guidance as to how the new penalties will be applied and how data controllers can appeal against the issue and amount of a penalty.

Note that during the consultations some respondents raised the concern that some organizations may be subject to 'double jeopardy', i.e.: being fined by both the FSA and the ICO for the same breach. Respondents should be assured that this is not likely to happen, as, on one side this is not technically possible, and, on the other, the ICO has confirmed so in the draft guidance.

The Personal Information Online Code

On 9 December 2009, the ICO published the consultation document on the personal information online code of practice (the "**Code**"). The Code provides good practice advice for all organizations involved in collecting and using personal data online. In summary, the Code requires organizations processing personal data online to be open and clear about such practices and ensure compliance with data protection laws.

The Code applies to activities such as collecting personal information through an online application form; profiling a website visitor by analyzing his online activity for example by using cookies; processing personal data for the purposes of online marketing; using cloud computing facilities for processing personal data and the international personal data transfers implications of using such facilities; and profiling individuals for other legitimate purposes.

The Code aims at clarifying when data collected via the use of cookies can be deemed to be personal data and who the data controller is in situations where more than one organization work together to provide a particular service. The Code also contains provisions in relation to vulnerable people such as children, the disabled and non-English speakers. In relation to subject access requests the Code questions whether these should also cover IP addresses and data collected via the use of cookies. The Code appears to conclude that these data should also be disclosed further to a subject access request unless there is an obvious privacy risk to third parties, which can occur where more than one individual uses the same computer.

The consultation is open until 5 March 2010 and can be accessed on http://ico-consult.limehouse.co.uk. Following the end of the consultation the ICO will publish a paper summarizing the responses and then the final version of the Code, which will provide helpful guidance to organizations processing personal data online.

If you would like to discuss any aspect of this alert or require further information on the matters referred to, please contact **Alastair Gorrie** on +44 (0)20 7862 4618 or **Lilly Taranto** on +44 (0)20 7862 4671.