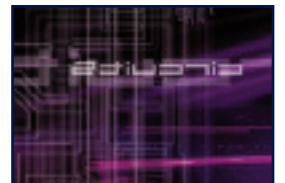
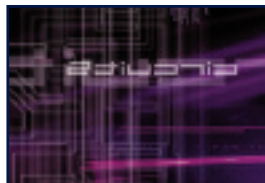


Data Protection Monthly Legal Update

July 2010

Title	Description
UK	
Information Commissioner's Office (ICO)	
<p>29 June 2010</p> <p>ICO publishes summary of responses to draft code of practice on assessment notices</p>	<p>In its summary of the responses to a consultation on a draft code of practice on assessment notices, the ICO said there had been a generally positive response to the approach of encouraging consensual audits, although there were also a number of concerns.</p> <p>For example, concern was expressed about the processes to be followed for compulsory and consensual audits. Following this feedback, the ICO has restructured the code to clearly identify the process for the audits.</p> <p>In addition, concern was expressed by private-sector organisations that the code did not appropriately consider differences between different work sectors and the roles of other regulators. In response, the ICO said that it would review and update the code as appropriate.</p> <p>The text of the summary can be accessed here.</p>
<p>30 July 2010</p> <p>ICO press release regarding taking pictures of school children at sports days</p>	<p>The ICO has issued a press release aimed at schools, reminding them that they cannot prevent parents from taking photos of their children at school sports days by virtue of data protection rules. The ICO encourages a common sense approach to photographs taken by family and friends at school events, where the Act is unlikely to apply.</p> <p>The Act however does apply where photographs are taken for official use by a school or college.</p> <p>Guidance released by the ICO can be viewed here.</p> <p>The press release can be viewed here.</p>



Title	Description
<p>7 July 2010</p> <p>ICO has published the Personal Information Online Code of Practice</p>	<p>The Information Commissioner's Office (ICO) has published the Personal Information Online Code of Practice to provide organisations with a practical approach to protecting individuals' privacy online.</p> <p>The Code gives advice on good practice, including discussion of online behavioural advertising; the approach that should be taken to collecting information from children online; the information that should be provided regarding privacy options on web browsers and websites; and what the default privacy settings should be. However compliance with the recommendations is not mandatory where they go beyond the strict requirements of the Data Protection Act 1998.</p> <p>Any business conducted online will be interested in the Code as it provides detailed information on the ICO's views on how the Data Protection Act applies in an online setting.</p> <p>You can access the Code of Practice here.</p> <p>Bird & Bird has written an article on the new Code. If you would like a copy of the full article, please contact Ruth Boardman (ruth.boardman@twobirds.com).</p>
<p>14 July 2010</p> <p>ICO publishes annual report for 2009/10</p>	<p>The Information Commissioner's Office (ICO) has published its annual report for 2009/2010, which includes information and statistics on the ICO's case work under the Data Protection Act 1998. The ICO received approximately 33,200 complaints concerning the DPA, a 30% increase over 2008/2009, with the largest volume of complaints being against the lending and direct-marketing sectors. The ICO stated that it will be reviewing its case-handling procedures to cope with this increase.</p> <p>The report can be accessed here.</p>
<p>Legislation</p>	
<p>6 July 2010</p> <p>Government issues call for evidence, seeking views on the DPA 1998 and Directive 95/46/EC</p>	<p>In light of the European Commission's plans to produce a legislative proposal reforming the Data Protection Directive (95/46/EC) before the end of 2010, the government has issued a call for evidence seeking views on the current law under the Data Protection Act 1998 and the Directive. It is intended that this exercise will place the government in a position to negotiate effectively for a new EU data protection instrument. Some of the questions raised by the call for evidence include whether the current data protection legislative framework provides sufficient protection in the processing of personal data, whether data controllers should be required to notify all data breaches to data subjects, whether the Information Commissioner's powers are adequate and whether the current arrangements for international transfers of personal data are effective.</p> <p>Responses to the call for evidence are requested by 6 October 2010.</p> <p>The government has also published a provisional post-implementation review impact assessment of the Act, on which it is also seeking comments.</p> <p>The call for evidence can be viewed here.</p>
<p>Enforcement</p>	
<p>18 June to 21 July</p> <p>Five undertakings signed</p>	<p>Undertakings were signed by five entities. See the table at the end of this update for details.</p>

Title	Description
Other	
<p>14 July 2010</p> <p>Home Secretary announces review of RIPA 2000</p>	<p>The Home Secretary has announced a review by the Home Office of counter-terrorism and security powers, which will consider the use of the Regulation of Investigatory Powers Act 2000 by local authorities and access to communications data more generally.</p> <p>The press release can be viewed here.</p>
Europe	
European Commission	
<p>Opinion of Advocate General Sharpston Joined Cases C 92/09 and C 93/09</p>	<p>Advocate General (AG) Sharpston has delivered an opinion on a reference from a German court. In her opinion, the AG considered that EU legislation which requires disclosure and publication on a publicly available and searchable website of the amounts awarded to farmers from Common Agricultural Policy (CAP) funds, together with their names, municipality of residence and postcode, was invalid.</p> <p>While the objective of achieving transparency in the management of CAP finance could, in principle, override the individual's fundamental right to respect for his private life and personal data, the AG concluded that neither the Council nor the Commission, who disagreed as to the purpose of publication, had put forward any plausible explanation.</p> <p>The full text of the opinion can be accessed here.</p>
<p>The Vice President of the European Commission gives speech at meeting of the Article 29 Working Party</p>	<p>Viviane Reding has given a speech at a meeting of the Article 29 Working Party on working 'Towards a true Single Market of data protection.' Viviane is responsible for Justice, Fundamental Rights and Citizenship.</p> <p>The text of the speech can be accessed here.</p> <p>The press release from the Article 29 Working Party can be accessed here.</p>
Cases	
<p>29 June 2010</p> <p>Commission v The Bavarian Lager Co Ltd, Case C-28/08</p>	<p>The ECJ has ruled that the European Commission was right not to disclose the full minutes of a meeting in October 1996 between the Commission, UK government officials and representatives of a trade association of European breweries. The court ruled that the applicant for disclosure had failed to establish the necessity of having the data transferred as required by Article 8(b) of the Data Protection Regulation.</p> <p>The full judgment can be accessed here.</p>

Title	Description
<p>Article 29 Working Party</p>	
<p>14 July 2010</p> <p>Article 29 Working Party releases FAQs relating to EU Commission Decision 2010/87/EU</p>	<p>The Article 29 Working Party has released a number of FAQs which address some of the issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.</p> <p>The FAQ document covers, amongst other issues, the following:</p> <ul style="list-style-type: none"> • The application of the Model Clauses; • The preferred legal framework for data transfers to a non-EEA sub-processor; and • The differentiation between sub-processing and additional data importers. <p>The FAQs can be viewed here.</p>
<p>13 July 2010</p> <p>Article 29 Working Party reports on compliance with Data Retention Directive</p>	<p>Following an investigation into member state's and electronic communications and internet service provider's compliance with the provisions of the Data Retention Directive (2006/24/EC), the EU Article 29 Working Party has adopted a report on an enforcement action.</p> <p>The investigation revealed significant discrepancies between member states for the categories and retention periods for internet data. As a result, the report makes several recommendations including:</p> <ul style="list-style-type: none"> • the list of traffic data to be retained under the Directive should be regarded as exclusive, so that member states could not impose additional data retention obligations; • there should be a single retention period shorter than the 24 months currently permitted; • service providers should be required to adopt common technical and organisational security measures; and • standardised procedures for handing data over to enforcement authorities should be adopted. <p>The report can be viewed here.</p>
<p>13 July 2010</p> <p>Article 29 Working Party Opinion 3/2010 on the principle of accountability</p>	<p>In the interests of having shared data protection values and principles, the Article 29 Working Party puts forward a proposal which would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with and organisations are held accountable for their failure to comply.</p> <p>The Opinion can be viewed here.</p>
<p>13 July 2010</p> <p>Article 29 Working Party Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing</p>	<p>Following review of the European Code of Conduct of FEDMA, the Article 29 Working Party is satisfied that the revised on-line marketing Annex for the use of personal data in direct marketing is in accordance with Directives 95/46/EC and 2002/58/EC and national legislation and provides sufficient added value. In particular, the Annex covers the on-line sector (e.g. the protection of children, unsubscribe facility) and therefore provides added value to the Directives by offering clear solutions for the questions posed in the on line marketing sector.</p> <p>The Annex, amongst other issues, addresses:</p> <ul style="list-style-type: none"> • How to obtain personal data directly from the data subject; • How to obtain data from sources other than the data subject; • Privacy policies and the use of cookies; • The protection of children; and • Forbidden practices. <p>The Opinion can be viewed here.</p>

Title	Description
<p>14 July 2010</p> <p>Article 29 Working Party issue press release regarding Data Retention Directive</p>	<p>Following a joint inquiry carried out by the data protection authorities, the Article 29 Working Party has released a report, which concludes that the obligation to retain all telecom and internet traffic data resulting from the European data retention directive 2006/24/EC is not applied correctly in EU member states.</p> <p>The full press release can be accessed here.</p>
<p>European Data Protection Supervisor (EDPS)</p>	
<p>EDPS calls for further data protection measures in draft SWIFT agreement</p>	<p>The EDPS has recommended that additional safeguards should be incorporated into the draft terrorist finance tracking agreement between the EU and the US (15 June 2010), including:</p> <ul style="list-style-type: none"> • requirements that bulk transfers of data from the EU to the US be replaced with mechanisms allowing financial data to be filtered so that only relevant and necessary data is transferred; • the retention period for non-extracted data be reduced from the five years currently suggested; and • any request by the US Treasury for access to the data be assessed by a public judicial authority. The draft agreement requires the consent of the European Parliament. <p>The full opinion can be accessed here.</p>
<p>EDPS Opinion on the proposal for a Council Decision concerning the mutual recognition of Authorised Economic Operator programmes in the EU and in Japan</p>	<p>The EDPS has handed down an opinion on the proposal for a Council Decision on a EU position within the EU-Japan Joint Customs Cooperation Committee concerning the mutual recognition of Authorised Economic Operator programmes in the EU and in Japan. The EDPS has recommended that the Commission:</p> <ul style="list-style-type: none"> • defines a conservation period for the personal data to be processed; • provides for mechanisms to guarantee the exercise of the rights of the data subject; and • establishes a procedure for the provision of information to the data subjects. <p>The opinion can be accessed here.</p>
<p>Other</p>	
<p>8 July 2010</p> <p>European Parliament approves SWIFT II agreement</p>	<p>The European Parliament has approved a long-term agreement on the processing and transfer of financial-messaging data from the EU to the US (SWIFT II agreement). The SWIFT II agreement will apply to the obtaining and use of financial-messaging and related data for the prevention, investigation, detection or prosecution of acts of terrorism or terrorist financing.</p> <p>SWIFT II has already attracted some criticism for its alleged inadequate protection of the privacy of EU citizens and for putting the EU in danger of economic espionage, contrary to the desires of the Article 29 Working Party, the European Data Protection Supervisor and the European Parliament.</p> <p>The agreement will initially be in force for five years and will automatically be extended for further periods of one year unless it is terminated by either party.</p> <p>The text of the Agreement can be accessed here.</p>
<p>12 July 2010</p> <p>Proposed Commission decision on adequacy of Israel's data protection laws</p>	<p>Ireland's minister of justice Dermott Ahern has expressed concern about the proposed Commission decision on whether Israel has adequate data protection. He has suggested that Israel must prove the status of its data protection principles. This objection follows an alleged forgery of Irish passports by Israeli security forces.</p>

UK

Enforcement Notices and Undertakings

Date	Entity	Enforcement notice or undertaking?	Data	Summary of steps required (in addition to the usual steps**)
18 June 2010	Chief Constable of Kent Police	Undertaking	Theft of documents containing personal data from a police officer's car. The officer had not used the secure briefcase provided to him and had not been provided with secure storage at his house contrary to the data controller's policies.	<p>Ensure that policies covering the transportation, storage and use of personal data are clarified and staff are made aware of their requirements.</p> <p>Ensure that relevant staff are provided with secure transportation and storage facilities.</p>
8 July 2010	London Borough of Barnet	Undertaking	<p>Theft of laptop, USB sticks and CDs from the home of an employee of the data controller. The devices contained the personal data of 9000 children and members of their family being schooled in the area. No password protection was in place and although the laptop was encrypted, the CDs and USB sticks were not.</p> <p>The employee had downloaded the data without authority of the data controller but enquiries revealed that staff had not received adequate training.</p>	<p>Ensure that devices containing personal data are encrypted using encryption software which meets the current standard.</p> <p>Ensure that all staff with access to personal data are made aware of the data controller's policies for the storage and use of personal data and are appropriately trained.</p> <p>Ensure that compliance with policies is closely monitored.</p> <p>Agree to an audit by the Commissioner later this year.</p>
8 July 2010	West Sussex County Council	Undertaking	<p>Theft of laptop from the home of an employee of the data controller. The device contained the personal data of an unknown number of children involved in child care proceedings.</p> <p>The employee had not received adequate security training and had not been shown how to access such files remotely.</p> <p>Enquiries also suggested that over 2000 unencrypted devices belonging to the data controller were likely in circulation.</p>	<p>Ensure that devices containing personal data are encrypted using encryption software which meets the current standard.</p> <p>Ensure that all staff with access to personal data are made aware of the data controller's policies for the storage and use of personal data and are appropriately trained.</p> <p>Ensure that compliance with policies is closely monitored.</p>
8 July 2010	Buckinghamshire County Council	Undertaking	<p>Loss of documents containing sensitive personal information of a number of children after a wallet was lost whilst stored in hand luggage in an airport.</p> <p>Enquiries also revealed that some of the data controller's policies including the staff training programme need revision.</p>	<p>Ensure that procedures are implemented to ensure that a proper risk assessment is carried out prior to the removal from the office environment of documents containing sensitive personal data, and appropriate security measures are adopted to protect such data in transit.</p> <p>Ensure that all staff with access to personal data are made aware of the data controller's policies for the storage and use of personal data and are appropriately trained.</p> <p>Ensure that compliance with policies is closely monitored.</p>

UK

Enforcement Notices and Undertakings

Date	Entity	Enforcement notice or undertaking?	Data	Summary of steps required (in addition to the usual steps**)
14 July 2010	Birmingham Children's Hospital NHS Foundation Trust	Undertaking	Two unencrypted laptops containing the personal data of 17 patients were stolen from the Medical Day Centre.	Ensure that adequate measures are put in place to ensure that data security policies are adhered to. Ensure that the unauthorised removal of encryption software against the data controller's security policies is prevented. Ensure that portable and mobile electronic devices, which are used to store and transmit personal data, are encrypted using encryption software which meets the current standard or equivalent. Ensure that physical security measures are adequate to prevent unauthorised access to personal data.

*The usual steps required of an entity are to give undertakings that:

1. Staff are made aware of the data controller's data protection policy and procedures, and are adequately trained on how to follow these; and
2. The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.

The content of this update is of general interest and is not intended to apply to specific circumstances. The content should not, therefore, be regarded as constituting legal advice and should not be relied on as such. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.

BIRD & BIRD

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 15 Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.

www.twobirds.com