SQUIRE PATTON BOGGS

WEEKLY DATA PRIVACY ALERT

11 August 2014

UK

ICO Warning to Legal Profession on Data Security

The Information Commissioner's Office (ICO) has warned the legal profession that it must keep personal data secure. Fifteen incidents involving barristers or solicitors have been reported to the ICO over the last three months. The ICO said that the regular use of paper files by lawyers increased the need for vigilance around data security. Also, the sensitive nature of the data handled by lawyers made it more likely that a monetary penalty would be imposed in respect of any breach. The ICO has produced some security tips for the legal profession.

ICO – News Release – 5 August 2014

Judicial Review of Data Retention and Investigatory Powers Act

Liberty, the UK organisation campaigning for fundamental rights and freedoms, has announced that it will seek judicial review of the new Data Retention and Investigatory Powers Act 2014 on behalf of MPs Tom Watson and David Davis. Liberty will argue that the treatment of the Bill as an emergency measure allowed no time for proper Parliamentary review and debate. It will also argue that the Act unjustifiably interferes with the fundamental rights to respect for family and personal life and the right to privacy and data protection guaranteed by the European Convention on Human Rights and the EU Charter of Fundamental Rights.

Liberty press release –July 2014

DMA Adopts New Code of Practice for Data Driven Marketing

The Direct Marketing Association (DMA) has adopted a new code of practice which must be followed by DMA members in respect of all data driven marketing activity. The new code is intended to address customer concerns about data privacy. It consists of five key principles and applies in addition to data protection laws. The code will come into effect for DMA members from 18 August.

DMA announcement – 4 August 2014 and DMA code of practice

France

CNIL Fine for CCTV Data Breaches

The French data protection authority, the CNIL, has imposed a fine of €5,000 on a retailer for breaches of the French Personal Data and Privacy Law in respect of its use of CCTV to monitor employees. In July 2013, the CNIL formally notified the retailer that it must inform its employees that they were being CCTV recorded and to cease using CCTV for permanent surveillance. The retailer subsequently informed the CNIL that it had complied with the notice. However, a fresh investigation four months later revealed that the data breaches were continuing. The CNIL found the €5,000 fine justified because of the continuing breaches despite the July 2013 notice and because the measures in place for keeping the data secure were inadequate.

CNIL Article – 1 August 2014

CNIL Closes Its Investigation Into Excessive Use of CCTV and Biometric ID Systems

The CNIL has closed its investigation against the French commercial centre LECLERC around its excessive use of CCTV devices and a biometric personnel identity system. The investigation was initiated following a complaint in April 2012 and the company corrected the data breaches identified after an on-the-spot check. The CNIL's President has confirmed that LECLERC's practices are now compliant with French Personal Data and Privacy Law, but has issued a reminder that any new breaches will be subject to penalties.

CNIL Article – 31 July 2014

CNIL Publishes New Insurance Fraud Norm

The CNIL has published a standardised norm for the processing of personal data to fight against insurance fraud. This completes the compliance pack for the insurance industry. The pack consists of several standard norms relating to the insurance industry and also includes practical information sheets. Companies in the insurance industry now have all the resources necessary for compliance with all the principles of data protection required by the CNIL.

CNIL notice – 31 July 2014

US

FTC Highlights Lack of Information on Data Collected by Apps

The Federal Trade Commission (FTC) has published a report highlighting that many of the most popular mobile shopping apps for consumers fail to provide adequate information on how consumer data will be handled. The FTC reviewed 121 different apps including those used for comparison shopping, redeeming deals and allowing consumers to pay in store using mobile devices. It found that, whilst most apps had a privacy policy, it was often vague and gave the app provider broad rights to collect and share a wide range of sensitive data. The report recommends that apps should clearly describe how they collect, use and share data and that app providers should put in place security measures to give proper effect to the terms of the privacy policy.

FTC – What's the Deal? An FTC Study on Mobile Shopping Apps – August 2014

FTC Approves COPPA Safe Harbour Program

The Federal Trade Commission (FTC) has approved the safe harbor program of iKeepsafe under the Children's Online Privacy Protection Act (COPPA). The FTC considered that the program provided the same or greater protections for children as those in COPPA itself.sensitive data. The report recommends that apps should clearly describe how they collect, use and share data and that app providers should put in place security measures to give proper effect to the terms of the privacy policy.

FTC Press Release – 6 August 2014

Court Rules That EU Data Must Be Handed Over to US Authorities

A US court has upheld an earlier ruling requiring Microsoft to hand over data held in its data centre in Ireland to the US government. The US government had obtained a search warrant requiring Microsoft to hand over certain data, including emails, stored at its premises. This latest ruling has confirmed that Microsoft is not only required to hand over data stored on US servers, but all relevant data regardless of its location. Microsoft has confirmed that it will appeal against the extra-territorial effect of the warrant on the basis that "people's email deserves strong privacy protection in the US and around the world".

Microsoft blog post – Microsoft responds to ruling in warrant case - July 2014

US Trustee Opposes Sale of Customer Data

In bankruptcy proceedings involving the US retailer Crumbs Bake Shop Inc (Crumbs), the US trustee has opposed the sale of Crumbs' customer lists on the basis that this would violate Crumbs' privacy policy. The privacy policy allows personal data held by Crumbs to be transferred only where this is required by government authorities, needed to provide services or following customer consent. The US trustee is arguing that the sale of the Crumbs business following bankruptcy does not fall within any of these three categories and should be prohibited unless a consumer privacy ombudsman is appointed by the bankruptcy court to ensure that the personal data is protected in the sale.

Australia

Australian Information Commissioner Publishes Security Guide Revisions

The Office of the Australian Information Commissioner has published revisions to the *Information Security Guide*, originally released in April 2013. The revisions have largely been prompted by changes to the Privacy Act 1988 introducing the Australian Privacy Principles. The revised guide provides information on the reasonable steps entities are required to take under the Privacy Act to protect the personal data they hold from misuse, interference and loss and from unauthorised access, modification or disclosure. The Commissioner is inviting comments on the revisions by 27 August.

Office of the Australian Information Commissioner announcement – Consultation information: Revised Guide to Information Security: 'Reasonable Steps to Protect Personal Information'– August 2014

Contacts

Mark Gleeson
T +44 20 7655 1465
E mark.gleeson@squirepb.com

Stéphanie Faber
T: +33 1 5383 7400
E: stephanie.faber@squirepb.com