SQUIRE PATTON BOGGS

WEEKLY DATA PRIVACY ALERT
18 AUGUST 2014

UK

Data Retention and Investigatory Powers Act

The Home Office has released its assessment of the privacy impacts associated with the interception provisions in the Data Retention and Investigatory Powers Act 2014 (DRIP). The Home Office has stated that the Regulation of Investigatory Powers Act 2000 (RIPA) places an obligation on anyone providing a service to customers in the UK, regardless of where the company's infrastructure is based. According to the Home Office, whilst these companies have always been bound by RIPA obligations, DRIP makes explicit the current interpretation of RIPA, and as a result there will be no new privacy risks associated with the new interception provisions.

Policy Paper: Data Retention and Investigatory Powers Bill – Interception provisions retention privacy impact assessment

Health and Social Care Information Centre (HSCIC) Data Pseudonymisation Review – Interim Report

The HSCIC's Director of Data and Information Services commissioned a review in November 2013 of the HSCIC's use of data pseudonymisation. The HSCIC published its interim report of the review on 31 July 2014. The review covers the use of pseudonymisation in respect of data in transmission to, received, held and disseminated by the HSCIC. The interim report sets out recommendations and options from the review to date, with the aim that the report will form the basis of the work of the Pseudonymisation Review Steering Group.

HSCIC Data Pseudonymisation Review – Interim Report – 31 July 2014

New Ofcom Guidance for Telecoms Providers

Ofcom has published new guidance for communications providers on their obligations under the Communications Act 2003. The Communications Act 2003 applies to telecoms providers and requires them to take measures to protect the security and resilience of their networks and services. Telecoms providers must notify Ofcom of a breach of security which has a significant impact on the operation of a network. The new guidance sets out steps to follow when deciding whether a security breach has had a "significant impact" and states that major incidents or incidents that are likely to generate media or political interest should be reported within 24 hours of commencing.

Ofcom guidance – 8 August 2014

Revised FLA Lending Code

The Finance and Leasing Association (FLA) have reviewed their Lending Code to ensure that it accurately reflects regulatory changes. The Code aims to give rights to customers who have taken out a consumer credit loan with an FLA member. The updated Code will come into operation from 1 October 2014. One of the key changes relates to the recording of health information, to ensure that the Code better reflects the requirement to obtain explicit consent and explain how the information will be used if recorded. The Code is not yet publicly available but will be accessible on the FLA website on 1 October 2014.

International

Brazil

The Brazilian Department of Consumer Protection and Defence (DPDC) Fines Internet Provider £900,000

The DPDC has fined Brazil's largest telecom company, Oi, BRL3.5 million (approx. £913,000) for failing to notify internet users that their browsing activities had been tracked and sold to third-party advertisers. The DPDC investigated allegations that Oi had developed an Internet activity monitoring program, which was being used to actively collect the browser data of broadband customers. This data was then sold by Oi to behavioural advertising companies without customers' consent. This is the first enforcement action to be brought by the DPDC since Brazil's internet law came into force in June 2014.

DPDC decision published 23 July 2014 (in Portuguese)

Ireland

Enforced Subject Access Now an Offence in Ireland

The Irish Minister for Justice and Equality has signed Statutory Instruments 337 and 338, bringing the remaining sections of the Data Protection Acts into force with effect from 18 July 2014. SI 338 brings into force section 4(13) of the Acts, which makes it unlawful for employers to require employees or applicants for employment to make an access request seeking copies of personal data which is then made available to the employer or prospective employer. This provision also applies to any person who engages another person to provide a service.

SI 337 of 2014

SI 338 of 2014

Irish Data Protection Commissioner (DPC) Issues Audit Guide

The DPC has power to carry out investigations in order to ensure compliance with the provisions of the Irish Data Protection laws. In order to assist organisations selected for audit, and to provide organisations holding personal data with a simple and clear basis to conduct a self-assessment of their compliance, the DPC has published guidance on the audit process.

http://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessAug2014.pdf

South Korea

Amended Personal Information Protection Act Now in Force

On July 30, 2013, the Korean Ministry of Security and Public Administration announced several amendments to the Personal Information Protection Act (PIPA). The amended PIPA came into force on 7 August 2014 and implements new strict penalties for failing to protect customer data, including fines of KRW100 million (approx. £60,000) and/or ten years' imprisonment. Companies are prohibited from collecting resident registration numbers but are awarded incentives, in the form of a reduction of corporation tax rates, if they invest in fighting cyber-attacks.

SQUIRE PATTON BOGGS

WEEKLY DATA PRIVACY ALERT
18 AUGUST 2014

Contact

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

14515/08/14