SQUIRE PATTON BOGGS

Weekly Data Privacy Alert
19 September 2016

UK

Brexit Continues to Cast Shadows Over UK Future

Japan has signalled its discomfort at the uncertainty looming over the UK's data protection legislation. Since the UK will no longer be bound by the existing EU legislation upon its eventual exit, Japanese businesses operating in the region fear potential difficulties in the transfer of data to and from the EU. This particularly affects ICT businesses with data centre operations in the UK, but also everyday transfers of data between parent companies and subsidiaries dispersed between the regions. This puts more pressure on the UK government to move forward in their negotiations with the EU and issue a clear plan for the future.

Japan's message to the UK and EU (PDF)

ICO Fines Two Companies a Total of £100,000

Acting on complaints received by people who had received large numbers of spam texts and calls, the ICO has fined Omega Marketing Services Ltd and Vincent Bond Ltd a total of £100,000. Omega Marketing Services Ltd, a company which sells solar panels and green energy equipment, made 1.6 million calls to people registered with the Telephone Preference Service, despite the fact that these people had not given their consent to receive such phone calls. Vincent Bond Limited, a debt management company, fell afoul of the ICO by sending 346,162 unauthorized spam texts. The monetary penalty notices for Vincent Bond Ltd and Omega Marketing Services are available online.

ICO investigations news

Information Rights Tribunal Reasserts Importance of Communicating Breaches to the ICO

Talk Talk Telecom's appeal in respect of the £1,000 penalty imposed by the ICO for delayed personal data breach was dismissed on 30 August. The matter concerned a Talk Talk customer who gained access to another person's personal data though an online facility. The ICO recommends that companies send a notification to them within the 24-hour deadline acknowledging the breach, as well as stating that an investigation is underway in accordance with Regulation 5A(2) of the Privacy and Electronic Communications Regulations 2003 and Article 2(2) of the European Commission Regulation No. 611/2013. They also expect to be kept regularly updated with details of the investigation. In this case, the customer complained on 18 November, but the ICO was only notified on the 1 December.

ICO judgment (PDF)

Germany

Bavarian Data Protection Authority Releases App Inspection Catalogue

The Bavarian Data Protection Authority (BDPA) has released a comprehensive inspection catalogue dealing with the technical data protection requirements surrounding apps and their development. The catalogue was developed on the basis of the practical inspection experience of the BDPA and best practice approaches stemming from the economy. The goal of the catalogue is to help app developers to comply with data protection requirements at an early stage and implement new concepts like Privacy by Design and Privacy by Default.

BDPA release (in German)

Federal Ministry of the Interior Considers Extending Data Retention to Messenger Services

Last week, the Federal Ministry of the Interior presented a new antiterrorism package, including an idea to overcome the legal distinction between telecommunication services and telemedia services. This change would mean that companies from both sectors could be subject to the same data retention legal requirements. This 2015 re-introduced and adjusted law on data retention would also be applicable to messenger services or social media. Currently, only telecommunication providers must retain data such as phone numbers, time and place of communication and IP addresses. This new law on data retention has, however, been brought before the Federal Constitutional Court.

Planned Measures to Increase Security in Germany (PDF) (in German)

Voßhoff Criticizes Ministers of the Interior for Plans to Extend Data Retention

Andrea Voßhoff, the Federal Data Protection Commissioner, has criticised a recent declaration by Christian Democrat Ministers of the Interior calling for a stricter security policy including the extension of data retention or video surveillance. Voßhoff acknowledged that preventing terrorist attacks is a big challenge, but warned that data protection and security should not be turned against each other. Voßhoff stated that security measures must conform to basic rights and data protection commissioners must be able to control the activities of security authorities.

BfDI Opinion on the "Berlin Declaration" (in German)

Berlin Data Protection Commissioner Criticizes State Use of "Silent SMS"

In a random assessment of the use of "silent SMS" (also called "stealth ping") by Berlin prosecution authorities, the Berlin Data Protection Commissioner has detected severe shortcomings in relation to aspects of its privacy. Silent SMS are messages that do not appear on the display of the mobile phone and trigger no acoustic signal. They can be used to locate a person and to create a precise movement profile.

According to the assessment, the sending of silent SMS was often not recorded properly or did not seem to be necessary. In most cases, the persons concerned had not been informed. The Commissioner thus called for a clearly defined legal basis for silent SMS in investigative procedures and a thorough control of this practice.

Article on Questionable Use of Silent SMS (PDF) (in German)

US

State AGs Weigh in on FCC's Proposed Rule

Sixteen state attorneys general (AGs) sent a letter to the Federal Communications Commission (FCC) on 9 September 2016, expressing concerns about the FCC's proposed rule, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services." The proposed rule is a follow-up to the FCC's 2015 Open Internet Order, which reclassified broadband providers (ISPs) as common carriers, subjecting them to Title II of the Communications Act. The proposed rule would establish new consumer privacy rules for consumers, and would only apply to ISPs and not to websites, applications or other "edge services."

The AGs expressed concern that the rule be construed "to pre-empt existing state laws that effectively protect consumers' privacy," and would "foster a Byzantine regulatory environment rather than clear, enforceable requirements that improve data privacy for all consumers." The AGs concluded that the proposed rule "is not conducive to better outcomes" in the context of the already existing complex regulatory environment, and urged the FCC to withdraw the proposed rule "and engage with the Federal Trade Commission and state Attorneys General to determine the most effective path forward to protect consumers and their privacy."

The FCC is expected to schedule a final vote on the proposed rule before the end of the year.

Contacts

Caroline Egan
Consultant, Birmingham
T +44 121 222 3386
E caroline.egan@squirepb.com

Annette Demmel
Partner, Berlin
T +49 30 7261 68 108
E annette.demmel@squirepb.com

Francesca Fellowes
Senior Associate, Leeds
T +44 113 284 7459
E francesca.fellowes@squirepb.com

Philip R. Zender
Partner, San Francisco
T +1 415 393 9827
E philip.zender@squirepb.com