SQUIRE PATTON BOGGS

WEEKLY DATA PRIVACY ALERT
2 MARCH 2015

EU

EU-wide Exchange of Cross Border Traffic Offenders Data

The EU parliament recently approved a draft law allowing for the exchange of data relating to traffic offenders between EU member states. The draft law will allow data to be shared between EU countries on drivers who commit traffic offences to help ensure that drivers who commit offences while abroad in the EU can be penalised. The new law is aimed at ensuring equal treatment of drivers across the EU. The changes approved by the Parliament provide a new legal basis (transport safety) for the data to be exchanged, as a previous draft law covering this issue was rejected by the European Court of Justice for lack of a legal basis. The old directive did not apply in the UK, Ireland and Denmark, but the change in legal basis means that they must put the new one into effect in their national laws within two years of its entry into force.

EU Parliament Press Release

MEPs Discuss Changes to Planned European Passenger Name Record (PNR) System

The EU Parliament civil liberties committee has been discussing a new draft text on an EU system for the use of Passenger Name Record (PNR) data. Among other issues, MEPs assessed the necessity and proportionality of the proposal, its scope, retention periods, the inclusion or exclusion of intra-EU flights, the connection with the on-going data protection reform, as well as the consequences of the EU Court of Justice judgement annulling the 2006 data retention directive. The deadline for MEPs to table amendments to the text is March 25.

EU Parliament Press Release

Netherlands

Dutch DPA Issues Advice on Draft Data Retention Law

The Dutch Data Protection Authority (DPA) has advice on a draft bill containing amendments to the existing data retention obligations for telephony and internet communications data. The draft bill follows a ruling in April 2014 by the Court of Justice of the European Union (CJEU), which found the EU Data Retention Directive (2006/24/EC) was invalid. The Dutch DPA found that the retention of the historical telephony and internet data of virtually all Dutch citizens for six to 12 months is a "far-reaching measure, requiring an irrefutable demonstration of necessity".

The Dutch DPA further stated that the infringement of the private life of virtually all Dutch citizens is too big and disproportionate. The Dutch DPA therefore recommended that the bill should not be presented to Parliament.

Dutch Data Protection Authority Press Release

UK

Privacy and Electronic Communications Regulations Published

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015 were published February 24, 2015. These Regulations make amendments to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (2003 Regulations). The first of these amendments is to permit certain providers of mobile electronic communications services to disregard restrictions on the processing of traffic and location data in the event of an emergency, that would otherwise be imposed on them by the 2003 Regulations. The second amendment is to lower the threshold at which the Information Commissioner may impose a monetary penalty, under the Data Protection Act 1998 as applied to the 2003 Regulations, for a serious breach of regulations 19 to 24 of the 2003 Regulations.

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015

Government Announces Plan to Target Nuisance Calls and Texts

The Government has announced that it will make it easier for the Information Commissioner (ICO) to impose financial penalties of up to £500,000 on companies making unwanted marketing calls and texts. Currently, the ICO can only issue monetary penalties of up to £500,000, if it is able to prove that marketing calls and texts sent by a company caused, or had the potential to cause, "substantial damage or substantial distress". The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015, bringing this change into effect, were published on February 24, 2015 and come into force on April 6, 2015. The Regulations now require that, for a monetary penalty to be imposed, the ICO must show that there has been a serious contravention of the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 and that (i) the contravention was deliberate; or (ii) the person knew or ought to have known that there was a risk that the contravention would occur but failed to take reasonable steps to prevent the contravention.

Department for Culture, Media and Sport Press Release

Enforced Data Subject Access Requests Prohibited

The Data Protection Act 1998 (Commencement No. 4) Order 2015 has brought into force section 56 of the Data Protection Act 1998. Section 56 introduces an offence which prohibits a person from requiring another person or a third party to make a subject access request and reveal the result. From March 10, 2015, companies will be banned from forcing individuals to request the disclosure of their personal information by third parties and requiring the individuals to share that information with them.

Data Protection Act 1998 (Commencement No. 4) Order 2015

ICO Fines Insurance Company £175,000 for IT Security Failings

An online holiday insurance company has been fined £175,000 by the ICO after it found that the company had breached the Data Protection Act 1998 after security flaws within its IT system let hackers access customer records. The hackers obtained credit card details of more than 5,000 customers and potentially had access to more than 100,000 live credit card details, as well as customers' medical details. The ICO investigation revealed that the company had no policy or procedures in place to review and update IT security systems, and had twice failed to update database software which could have prevented this incident.

ICO Press Release

US

Director of National Intelligence Highlights the Growing Issue of Cyber-attacks

James Clapper, the Director of National Intelligence, has warned in his opening statement on the worldwide threat assessment before the Senate Armed Services Committee that cyber-attacks against the US are increasing in frequency, scale, sophistication and severity of impact. He further stated that the US has been living with "a constant barrage" of cyber-attacks for some time. James Clapper concluded that this trend is set to continue and that the methods of attack, the systems targeted and the victims are continuing to expand in diversity and intensity.

James Clapper speech

For further information on any of the items in this week's alert, please contact:

Mark Gleeson (London)
Partner
T +44 207 655 1465
E mark.gleeson@squirepb.com

Annette Demmel (Germany)
Partner
T +49 30 7261 68 108
E annette.demmel@squirepb.com

Mark D Johnson (US)
Senior Attorney
T +1 202 626 6265
E mark.johnson@squirepb.com

16659/03/15