SQUIRE PATTON BOGGS

Weekly Data Privacy Alert
27 February 2017

EU

MEPs Vote to Increase the Protection of Data Collected at EU Borders

Civil Liberties MEPs recently voted to shorten the retention period for data gathered under the new EU entry/exit system for non-EU nationals and to introduce measures that strengthen the protection of such individuals' data. The new system is electronic and replaces the procedure of individuals having their passports stamped. The Commission hopes that storing travellers' data electronically will help identify persons who overstay their visas or perpetrate identity fraud. MEPs voted to reduce the period for which data is stored to two years as compared with the five years originally proposed by the Commission. MEPs also voted to approve measures designed to ensure that the new system is compliant with the General Data Protection Regulation, with individuals having a right to access their data. MEPs are expected to enter into negotiations with the European Council regarding the proposed amendments in March 2017.

France

French Data Protection Authority Launches RFP for a Privacy Impact Assessment Tool

The French data protection authority (CNIL) has launched an RFP under public procurement rules for a Privacy Impact Assessment software tool (assistance with project management and the development of the software). The tool is meant to be used by all data controllers in France and has to be compatible with all operating systems. The CNIL has indicated that the tool will potentially be used at the EU level and that the interface will, therefore, have to be multilingual so that it can be adapted to the different official languages of the countries of the European Union. The first version of the tool will use French or English. The solution is intended to be published under a free licence, recognised as such by the Free Software Foundation or the open source initiative, at the discretion of the CNIL. The deadline for submission is 29 March 2017 at 5 p.m. French time.

French Data Protection Authority Launches Consultation

The French data protection authority (CNIL) has launched a new online consultation on data breach notifications, consent and profiling (topics that are based on Article 29 Working Party's most recent action plan). The consultation will be open from 24 February 2017 until 24 March 2017. The CNIL will organise a workshop in Brussels after the responses to the consultation have been received.

Conseil d'Etat Requests Preliminary Ruling from CJEU on Right to be Forgotten

The *Conseil d'Etat* has requested preliminary rulings from the Court of Justice of the European Union (CJEU) in relation to a number of cases concerning the implementation of the right to be forgotten. In particular, the *Conseil d'Etat* queried the obligations which apply to search engine operators in relation to websites that contain sensitive personal data.

In referring its questions to the CJEU, the *Conseil d'Etat* highlighted the collection and processing of data relating to sexual orientation, political, religious or philosophical opinions, criminal offences, convictions or safety measures as an area which required greater clarity. The cases brought before the *Conseil d'Etat* raise questions that are closely connected with the obligations of a search engine operator when such information is embedded in a press article or when the content that it relates to is false or incomplete.

Germany

European Commissioners for Freedom of Information Issue Common Resolution in Berlin

The German Federal Data Protection Commissioner, Andrea Voßhoff, recently welcomed the European Commissioners and Ombudsmen for Freedom of Information at a two-day conference in Berlin. The conference resulted in a common resolution, which was adopted on 24 February 2017. The resolution states that Europe is in need of common standards for freedom of information, which should be fostered in a constructive dialogue between commissioners, ombudsmen, parliaments and governments. The participants of the conference appealed to European parliaments and governments to guarantee the right of every individual to information access vis-à-vis independent and adequately equipped institutions.

Berlin Data Protection Commissioner Offers Extra Consulting Hours for Start-Ups

From 1 March 2017, the Berlin Data Protection Commissioner, Maja Smoltczyk, will offer cost-free consulting hours with an emphasis on providing support for start-ups. Smoltczyk will offer consultancy services regularly every first and third Wednesday of the month from 2 p.m. to 4 p.m. The background to this initiative is to support the image of Berlin as a "start-up-city". Smoltczyk stated that she wants to assist new companies to adopt privacy measures at an early stage in order to help them avoid cost-intensive rectifications and to make good business decisions. Common topics are expected to include privacy measures concerning tracking and profiling, as start-ups typically deal with the development of software and data analysis for optimizing business models and products.

Data Protection Authorities Call for Enhanced Privacy in Amending the Identity Card Act

In the course of the planned amendment of the Identity Card Act (*Personalausweisgesetz*) by the German Federal Government, the Conference of the Independent Data Protection Authorities of the *Bund* and the *Länder* (the Conference) has called for reform to take better account of civil and data protection rights. One of the Conference's main criticisms related to the current plan for the obligatory activation of the online function of electronic identity cards. Such a solution could only be considered lawful if citizens have the right to decide whether electronic identification can be used. The Conference also criticised the allocation of authorisation certificates to service suppliers and the almost unconditional right (to be introduced from 2021) of the police and secret services to access ID photographs through an automated process.

UK

ICO Releases Guidance for Consent in the GDPR

On 2 March 2017, in preparation for the new EU General Data Protection Regulation (GDPR) coming into force on 25 May 2018, the Information Commissioner's Office (ICO) released its draft guidance on consent for public consultation. The draft guidance makes it clear that obtaining valid consent under the GDPR will be significantly more difficult than under the current law. In particular, it expressly states that "opt-out" consents will no longer be valid and that businesses will need to obtain positive "opt-in" consents in order to comply with the GDPR. In addition, third party consents will only be valid if the third party sending the marketing was specifically identified in the consent wording. As it currently stands, the guidance is likely to require the majority of businesses to go out and seek new consents in order to continue their marketing activities post the GDPR coming into force. This is not only due to the need for specific, opt-in consents, but also due to the obligation to be able to demonstrate that consent has been obtained. Businesses will need to be able to prove when and how consent was obtained and what information individuals were given at the time. Many businesses will not have these detailed records. The take-up for new consents is notoriously low, which could hit revenues hard. The consultation will run until 31 March 2017 with the ICO aiming to publish the finalised guidance in May 2017.

ICO Fines Credit Broker for Sending More Than Five Million Unlawful Text Messages

The ICO has fined the credit broker Digitonomy Ltd £120,000 for sending millions of marketing SMS messages without appropriate consent. Digitonomy used affiliate marketing companies to conduct a marketing campaign in which they sent out messages offering cash loans. Digitonomy relied on the consent wording of the affiliates, which did not set out that by providing their data consumers consented to the receipt of direct marketing via text message. On that basis, the ICO found that the text messages had been sent without proper consent and so were unlawful.

US

FCC Stays Implementation of Data Security Requirements for Telecommunications Carriers, Including Internet Service Providers

The Federal Communications Commission (FCC) voted 2-1 today to stay the implementation of requirements approved last year that mandate that telecommunications carriers, including ISPs, take "reasonable measures to protect customer [proprietary information] from unauthorized use disclosure or access". Under the FCC's reclassification decision, ISPs are now "telecommunications carriers" for certain aspects of the Communications Act. The data security requirement, which was a component of an extensive set of privacy rules adopted by the FCC prior to President Trump's election, was to have taken effect on 2 March 2017. The Republican Commissioners, now the majority, had both voted against the adoption of those rules. In a news release, the FCC stated, "the Commission's stay will provide time for the FCC to work with the [Federal Trade Commission] to create a comprehensive and consistent framework for protecting Americans' online privacy. The Federal Trade Commission had proven to be an effective cop on the beat for safeguarding digital privacy." This may be but the first step in likely regulatory surgery on the FCC rules, the real substance of which are not scheduled to take effect until later this year. In the meantime, the Commission noted that "ISPs have been – and will continue to be – obligated to comply with Section 222 of the Communications Act and other applicable federal and state privacy, data security, and breach notification laws. In addition, broadband providers have released a voluntary set of 'ISP Privacy Principles' that are consistent with the Federal Trade Commission's long-standing privacy framework." For other telecommunications carriers, the Commission's pre-existing rules governing data security will remain in place.

Contacts

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

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

Stephanie Faber
Of Counsel, Paris
T +33 1 5383 7400
E stephanie.faber@squirepb.com

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

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

Emma Garner
Associate, Leeds
T +44 113 284 7416
E emma.garner@squirepb.com