SQUIRE PATTON BOGGS

Weekly Data Privacy Alert

25 July 2016

EU

EU Commission Adopts EU-US Privacy Shield

Following support from the majority of EU Member States, the European Commission has issued an adequacy decision formally adopting the EU-US Privacy Shield. The framework arrangement was finalised with the US Department of Commerce in June of this year and concerns measures aimed at legitimising the trans-Atlantic transfer of European personal data to the US. The long awaited Privacy Shield replaces the old Safe Harbor framework, which was invalidated by the European Court of Justice in October 2015.

As well as imposing tougher obligations and more rigorous procedural requirements on US companies handling data relating to European citizens, the Privacy Shield safeguards and adds transparency obligations in relation to the US government's access to transferred data. It includes new rules requiring the deletion of data and places limitations on onwards transfers to third parties. The new arrangement also provides a free dispute resolution mechanism allowing European citizens to raise complaints about the abuse of their personal data, creates an independent US Ombudsman to address these concerns and implements an annual joint review mechanism in order to monitor its ongoing functionality.

The Department of Commerce will begin accepting certifications of compliance from 1 August. While several US companies have already publically indicated their intent to apply for Privacy Shield status, it is likely that the arrangement will face further challenges in the courts by those who believe that it does not provide sufficient improvements to the Safe Harbor regime, particularly in relation to mass surveillance by US law enforcement and national security agencies.

Press release

European Data Protection Supervisor Publishes Background Paper on Necessity

The European Data Protection Supervisor (EDPS) has published a Background Paper intended to develop an approach for assessing the necessity of measures that interfere with the fundamental rights to personal data protection and the respect of private life. In forming its recommendations, the Paper draws on various sources of European case law, previous opinions of the EDPS and the Article 29 Working Party, and from the Charter of Fundamental Rights of the European Union Charter in which these rights are enshrined. The Paper provides that "[t]he test of necessity should be considered as the first step with which a proposed measure involving processing of personal data must comply," and proposes a six-step checklist to implement that test.

Background Paper (PDF)

European Privacy and Consumer Organisations Write Letter to EU Commission Concerning Data Protection in TiSA and TTIP

In an open letter to the European Commission, the European Consumer Organisation (BEUC) and European Digital Rights (EDRi) have expressed deep concern with regard to recent information that the US government is opting for a full prohibition of data localisation policies in the Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA). The organisations have asked the Commission to publically state that it will not support such provisions in the context of trade agreements on the basis that data and privacy issues should remain separate from any trade negations.

Open Letter (PDF)

Germany

Data Protection Commissioner of Nordrhein-Westfalen Publishes Booklet on Self-Data Protection

The Data Protection Commissioner of Nordrhein-Westfalen and a regional consumer organisation (*Verbraucherzentrale Nordrhein-Westfalen*) have published a booklet on self-data protection and data economy. The booklet provides details of the privacy risks of scoring, credit agencies, social networks and fitness trackers. It also makes recommendations for precautionary measures such as deactivating cookies, carefully reviewing privacy policies, requesting information from companies or the eventual withdrawal of consent.

Self-data protection booklet (in German)

Commissioners for Freedom of Information: All Federal States Should Participate in the Data Portal "GovData"

The German Federal Data Protection Commissioner, Andrea Voßhoff, has welcomed an appeal by the German Conference of Commissioners for Freedom of Information inviting all federal states to participate in the data portal GovData. GovData provides access to open administrative data for reasons of transparency and efficiency, a system which until now had only be adhered to by the "Bund" and nine "Länder".

Press release (in German)

Bundestag Adopts Anti-Terrorism Package

The German Bundestag has adopted a draft law for the improvement of information exchange in combating international terrorism. Aside from extending the capabilities of the Federal Office for Protection of the Constitution and the Federal Police, the law also tightens the provisions of the German Telecommunications Act obliging telecommunication providers to process and store personal data of customers. Interestingly, an application to the European Court of Human Rights filed in 2012 against these provisions is likely to be held admissible. This follows from a recent Court letter informing the applicant that the German government has been asked to make a statement on the admissibility and merits of the case. The application in question concerns whether or not the prohibition of anonymous mobile communication is compatible with the rights to private life and freedom of expression under the European Convention on Human Rights (Articles 8 and 10 respectively).

Press release (in German)

US

US Federal Government Release Final Guidance on Cybersecurity Information Sharing Act of 2015

The US Department of Homeland Security (DHS) and the US Department of Justice (DOJ) have issued joint guidance on the Cybersecurity Information Sharing Act of 2015 (CISA). The CISA, which was enacted in December 2015, includes a number of measures aimed at reinforcing public and private sector cybersecurity. The final guidance focuses on the sharing of "cyber threat indicators" and "defensive measures" which operate under the Act. Through CISA's information-sharing initiative, the federal government has the power to gather known cyber threat indicators and defensive measures, which will then be made available to other federal agencies, select private entities and to the public, if unclassified in nature. Participating entities, including private companies, must ensure that the information they share is scrubbed of personal information or of any information identifying a specific person not directly related to a cybersecurity threat.

Privacy and Civil Liberties Final Guidelines (in German) and Final Procedures (PDF)

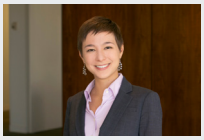
Contacts

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

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

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

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



Martha Wrangham
Associate, Denver
T +1 303 894 6115
E martha.wrangham@squirepb.com