ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Safe Harbor invalid: What to expect after the ruling?

Sarah Cadiot and **Laura De Boel** explain what businesses can do to enable transfers to the US.

On 6 October 2015, the Court of Justice of the European Union (CJEU) issued a landmark judgment[1] invalidating the European Commission's Decision of 2000[2] which recognised the adequacy of the EU-U.S Safe Harbor framework (Safe Harbor). In addition to the invalidation of this adequacy decision, the CJEU upheld the power of national Data Protection Authorities (DPAs) to independently investigate international data

Continued on p.3

ECJ clarifies meaning of territorial scope in DP Directive

Hungarian data protection law applies to a company's activities in Hungary, although registered in Slovakia. **Andrea Klára Soós** reports.

On 1 October 2015, the European Court of Justice (ECJ) published its decision in case No. C-230/2014[1]. In this decision the ECJ followed the argumentation of Advocate General Pedro Cruz Villalón[2] and came to the conclusion that the principle of establishment should be applied by the authorities of other EU Member States. Consequently, a data controller could be investigated

Continued on p.5

Issue 137 **October 2015**

INTERNATIONAL report

ISSUE NO 137 **OCTOBER 2015**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Sarah Cadiot and **Laura De Boel**
Wilson Sonsini Goodrich & Rosati, LLP, Belgium
Andrea Klára Soós
Soós law firm, Hungary
Hiroshi Miyashita
Chuo University, Japan
Yuli Takatsuki and **Phil Lee**
Fieldfisher Silicon Valley, US
Whon-il Park
Kyung Hee University Law School, South Korea
Patricia Muñoz-Campos
Bird & Bird, Spain
Andra Giurgiu
University of Luxembourg, Luxembourg
Gertjan Boulet and **Paul De Hert**
Vrije Universiteit Brussels, Belgium
Colin J. Bennett
University of Victoria, BC, Canada
Sinta Dewi Rosadi
Padjadjaran University, Indonesia

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Safe Harbor collapses – but data transfers will continue

The Court of Justice of the European Union's recent landmark decisions on Weltimmo and Safe Harbor (p.1) strengthen individual Data Protection Authorities' powers. The EU DPAs can now make decisions whether to suspend transfers to the US – but the EU Commission immediately said that a coordinated approach is needed to avoid fragmentation. The Chair of the Article 29 DP Working Party, Isabelle Falque-Pierrotin, President of France's CNIL agreed – but will all DPAs share this view? DPAs now have to come up with a plan of action for now until a new regime for EU-US transfers can be agreed.

The EU Commission says that it will step up negotiations with the US on 'Safer Harbor' and is still confident that the EU Data Protection Regulation can be agreed this year. One aspect of the reform is the ambitious plan for a One-Stop-Shop (p.16). It will require enhanced cooperation between the regulators – something that is already taking place on Binding Corporate Rules and, to some extent, within the DPAs' enforcement network (p.19).

The court's decision in the Weltimmo case (p.1) states that DP law of a Member State may be applied to a foreign registered company if it has activities in a country, for example, operating in the native language of the country and has representatives in that country, even if not headquartered there. This decision is likely to have a huge impact on companies operating on the Internet. The Safe Harbor / Max Schrems case is essentially about US surveillance with major impact on transfers (p.1). Key US legal provisions are discussed from p. 11 onwards.

The nearly adopted Umbrella Agreement signifies an important step in rebuilding trust in EU-US data flows. However, the European Parliament's approval is still needed and it has not been satisfied with the secretive negotiation process (p.7). The same secrecy surrounds the EU DP Regulation Trilogue process – there is no information in the public domain.

Asia is on the world privacy map now due to its Big Data related actions. Read about Japan's new law (p.8) which is intended to win it EU adequacy status, while South Korea's initiatives are in the context of its "Creative Economy" business synergy programme (p.15). In addition, there is a new Indonesian draft regulation, which affects both private and public sectors (p.27). By contrast, India's Supreme Court may play a role in making progress on a timetable for an ID card-related privacy law but the slow and confusing turning of legal wheels means that an Indian privacy law looks likely to be delayed until an unknown future (p.24).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Indonesia issues draft Ministerial Regulation on Data Protection

By **Sinta Dewi Rosadi**.

Although mobile traffic data usage is likely to increase nine-fold by 2020,[1] in Indonesia the legal protection for such digital-based activities is still weak. Currently there are no specific rules that ensure the protection of users' data privacy. With a wide range of applications, users are asked to provide their address, mobile phone number and credit card number – and those details will be recorded. No less important is that data controllers process data on transactions, travel routes, user habits, patterns of communications and data about user activity in the context of a variety of applications or Internet pages. To address these developments, Indonesia's Ministry of Communications and Informatics (Infocom) has drafted Ministerial Regulations on Personal Data Protection (PDPES) in Electronic Systems as an implementing regulation based on Government Regulation No. 82/2012 on Electronic Transaction Systems.[2] Ministry regulations are a lower form of legislation than Government regulations or Acts of Parliament. The PDPES will cover basic protection mechanisms such as the rights of data subjects, user liability, liability for operators of electronic systems, dispute resolution, public participation and administrative sanctions. A public consultation was completed in July, but it is not certain when the final Regulation will be released.

The draft regulation deserves attention because for the first time the government of Indonesia will issue a specific regulation on protection of personal data. However, it is regrettable that PDPES will overlap with the Personal Data Bill being prepared by another Directorate in Infocom. A ministerial regulation is not compatible with Indonesia's Constitution, according to which personal data protection is part of the Privacy Right which is protected by the Constitution and considered as a fundamental right, therefore requiring an Act[3] rather than the lesser form of a Ministerial Regulation. It may also be criticised on other grounds. The PDPES does not clearly stipulate its scope (individuals or legal entities; public and/or private sectors), although it does only apply to 'Electronic System Operators'. The regulation only applies minimum basic data protection principles such as consent, right to verified content, and right to access and correction. The regulation requires data subjects' written consent, but does not clearly stipulate whether the mechanism to be used is opt-in or opt-out.

The data retention period is long under PDPES (5 years); this is in accordance with the National Retention Schedules Regulation in the National Archives Law, which was developed to regulate the public archive, not personal data.

There is no specific rule in PDPES that gives authority to a state institution to supervise this system. To effectively implement legislation, a supervision mechanism would be required, as well as a legal instrument which governs personal data protection.[4]

According to the 'data localisation' requirement in the draft governmental regulation (under which this ministerial regulation is made) the 'data centre and disaster recovery centre' must be located on Indonesian territory. This draft is still tentative because the Ministry is in the process of receiving input from the public.

The Draft Ministry Regulation will operate as follows[5]:

1. Protected personal data

Personal data refers to any true and real information that can be directly or indirectly identified as relating to an individual, to be used in accordance with existing regulation.

2. Data collection and processing

The PDPES includes protection of the collection, processing, analysing, storing, notification, transmission, dissemination and destruction of Personal Data.

Personal data shall be processed only if:

(a) Data subjects have given their consent
(b) Personal data obtained and collected directly must be verified by the data subject
(c) Personal data obtained and collected indirectly must be verified based on various sources
(d) Personal data may only be processed and analysed according to the needs/purpose of the Electronic Systems Operator that have been stated clearly when obtaining and collecting the data.

3. Retention

Electronic Systems operators may store personal data for 5 years or more or in accordance with applicable regulations.[6]

4. Responsibility of electronic system administrator/management

Each Electronic System Operator must have internal rules to carry out the process and ensure the protection of personal data.

5. The rights of data subjects:

a. The confidentiality of their personal data
b. The right to file a complaint with the personal data dispute resolution institutions for failure of personal data confidentiality protection by the Operator Electronic Systems, and the right to sue in a civil court
c. The right to reclaim one's personal data, when the services of an Electronic System Operator are no longer needed
d. The right to access and the opportunity to change or update personal data without disturbing personal data management systems.

6. The responsibility of data controllers

a. To maintain the confidentiality of personal data that it has obtained, collected, processed and analysed
b. To process personal data only in accordance with the purposes for which it was collected