# Academics propose law and policy requirements for deployment of privacy indicators

A research paper by US academics offers criteria that can be established in law and policy so that trustworthy and meaningful privacy indicators can be successfully deployed and adopted through technological tools.

These tools are needed – the GDPR suggests the use of "standardised icons in order to give, in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Also in the US, the Federal Trade Commission (FTC) has stressed the importance of improved notice as a means for providing greater transparency.

Privacy policies are often long and too complex for consumers to understand. There have been developments in labels, icons (p.16), privacy certifications, seals and privacy dashboards, but many challenges remain. The authors say that one of the problems is that "The lack of standardization prevents user-recognizability and dependability in the online marketplace, diminishes the ability to create automated tools for privacy, and reduces incentives for consumers and industry to invest in privacy indicators."

The authors say that indicators can adequately, accurately, and successfully synthesize online privacy content if:

1. lawmakers or regulators establish standardized evaluation criteria as to the privacy practices to be considered and how these should be weighted in scoring techniques;

2. in the analytical and interpretive approach, rating mechanisms deployed by industry convey to users actual and demonstrable data practices, or simply show what a privacy statement says regarding recognized criteria rather than make deductive conclusions, and tools align with legal principles of contract interpretation and legal defaults as to the meaning of silence in privacy policy language;

3. a standardized system of icons is developed through government and industry collaborations, along with guidelines as to where these should be presented; and

4. privacy raters are impartial, honest, autonomous, and financially and operationally durable.

• *The paper, 'Trustworthy privacy indicators: grades, labels, certifications, and dashboards', by Joel R. Reidenberg, Professor of Law, Fordham University Law School, and his colleagues from Fordham Center on Law and Information Policy (CLIP), is at papers.ssrn.com/sol3/papers.cfm?abstract_id=3342747*

# South Africa's personal data law in force soon

Speaking at the CPDP conference in Brussels on 23 January, *Sizwe Snail*, Commissioner at South Africa's Information Regulator said that the 2013 Protection of Personal Information Act will now finally enter into force in the second quarter of 2020. The regulator has been established for three years and consists of five members, who enforce both data protection and freedom of information law.

The CPDP panel on BRICS countries (Brazil, Russia, India, China and South Africa) discussed international harmonisation of data protection networks. *Bruno Gencarelli*, Head of International Data Flows and Protection Unit at the European Commission, said that unlike in many other areas, convergence is real and happening. Data protection is no longer seen as a European obsession, he said. Our system is based on a high level of protection and openness to data flows, we see these two elements as complementary. That is why we are keen to work even more intensively with countries seeking adequacy.

Professor *Luca Belli* of Rio Law School in Brazil said that all of the BRICS countries, apart from Russia, have included the possibility of adequacy decisions in their data protection frameworks.

Brazil's privacy law will be in force in August 2020, and the supervisory authority is being appointed shortly. An unofficial English translation of the law is now available at cyberbrics.info

• *CPDP is organising a Latin American Data Protection conference in Brazil 23-25 June 2020.*
*See www.cpdpconferences.org*

# UK ICO delays fines on BA and Marriott

Last July, the UK ICO issued Marriott International and British Airways with a notice of intent to issue a penalty. On 21 November, the ICO announced that "both entities made representations to the Information Commissioner regarding these notices in accordance with Schedule 16, paragraph 3(3) of the Data Protection Act 2018. The Information Commissioner is considering those representations in deciding whether to give a penalty notice, and the amount of the penalty if a penalty notice is given."

The period for giving a penalty notice to a person may be extended by agreement between the Commissioner and the data controller or data processor.

The ICO is currently considering the representations that have been made by both companies. It has been reported that the deadline would now be 31 March.

• *See ico.org.uk/about-the-ico/our-information/disclosure-log/enq0889841/*

 