pdp JOURNALS

ISSN 2049-5307

Privacy & Data Protection

Volume 21, Issue 4 March 2021

Headlines

- e-Privacy Regulation progresses to next stage, p.18
- Amendments to Singapore's Personal Data Protection Act now in force, p.19
- EDPB answers key questions on health research data, p.20

Contents

New EU guidelines on breach notification

The European Data Protection Board has published draft guidelines ('the Guidelines') for data breach notification, giving helpful clarity on the scope of organisations' notification and remediation obligations under the GDPR.

The Guidelines reflect the shared experiences of Supervisory Authorities since the GDPR became applicable. Addressing six common types of personal data breach — ransomware, data exfiltration attacks, internal human risk, lost or stolen device and paper documents, misposted data, and social engineering attacks — the Guidelines contain 18 case studies illustrating what the EDPB considers 'appropriate risk assessment' and resulting notification obligations for each category of breach.

In terms of general guidance, the Guidelines remind organisations that they should notify SAs of relevant data breaches without undue delay. In high-risk cases, notifying a data breach within the 72-hour timeframe provided by the GDPR may be unsatisfactory. For certain cases which are not high-risk, organisations should notify data subjects in addition to regulators as a best practice.

The Guidelines give examples of when notifying individuals is advisable and when it is necessary.

The Guidelines state that breaches involving Special Category data do not automatically result in an obligation to notify individuals. Organisations should assess the risks and impacts triggered by the breach (e.g., potential detrimental use or connotation of the data) to determine whether to notify.

The case study dealing with ransomware attacks shows the EDPB's think-

(Continued on page 17)

UK close to securing adequacy

The EU Commission has issued draft adequacy decisions for transfers of personal data to the UK, one under the GDPR and the other for the Law Enforcement Directive.

The publication of the draft decisions is the beginning of a process which involves obtaining an opinion from the European Data Protection Board, and then securing the 'go ahead' from a Committee composed of representatives of the EU Member States. Following this, the Commission can proceed to adopt the two adequacy decisions.

Both the government and the UK Information Commissioner have issued statements welcoming the development.

Rafi Azim-Khan, Head of Data Privacy at Pillsbury law, commented: "You could probably power the UK's entire offshore wind fleet with the sigh of relief from UK businesses following the data adequacy finding. The internet and e-commerce platforms are, by their very nature, borderless, and UK businesses of all shapes and sizes did not want to see prohibitions (or the cost and complexity of having to put in place contractual arrangements to cover each data transfer) for handling data from the EU. Failing to grant adequacy would essentially

(Continued on page 17)