pdp® JOURNALS

Data Protection Ireland

Volume 14, Issue 2 March / April 2021

Headlines

- DPC clarifies meaning of CCTV decision, p.18
- DPC criticised for weak IT systems, p.19
- Online Safety Bill soon to undergo pre-legislative scrutiny, p.20

Contents

e-Privacy Regulation progresses to next stage

Following the EU Presidency's release of a new draft of the ePrivacy Regulation (see page 1 of the last issue of this journal), the Council of the EU's Permanent Representatives Committee has adopted an agreed position on the ePrivacy Regulation. The legislation can now progress to the next stage of negotiation (the trilogue stage).

Among the key positions taken in the draft is the position on 'cookie walls' (where an end user is prevented from using a service unless they have accepted a form of cookie). The draft does not prevent cookie walls, and provides that access to a free service can be made conditional on accepting cookies, provided that the service provider offers an equivalent option that does not require the acceptance of cookies.

In terms of direct marketing, there is little substantive change in the new draft from the previous draft. Member States are empowered to determine their own period of time after which direct marketing consents will be effective or expire, and assign call identification prefixes to identify direct marketing calls.

The draft allows for processing of metadata without consent for certain defined purposes. These relate to information security, fraud prevention, service provision (for example, billing and managing abuse of the service) or for the protection of 'vital interests' which follows the same concept used in the GDPR.

The draft provides for an exception from the requirement to obtain consent and to delete or anonymise device data and/or metadata once they are no longer needed to provide the-

(Continued on page 17)

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.

(Continued on page 17)