pdp JOURNALS

ISSN 2049-5307

# Privacy & Data Protection

Volume 21, Issue 1 October / November 2020

## Headlines

- ICO's new guidance on DSARs may move needle in favour of employers, p.18
- EU Parliament wants tighter rules on behavioural ads, p.19
- CNIL makes targeted advertising a priority, p.20

## Contents

*Expert comment* 2

*The Age Appropriate Design Code* 3

*Data processing addenda* 8

*Learning from others' mistakes: two common security failings in five data breaches* 12

*News & Views* 17

## ICO consults on monetary penalty decision-making

The UK Information Commissioner's Office has launched a consultation on draft Statutory guidance which details how it will regulate and enforce data protection legislation in the UK.

A requirement of the Data Protection Act 2018 ('DPA'), the guidance explains how the ICO will exercise its regulatory functions when issuing information notices, assessment notices, enforcement notices and penalty notices.

The guidance outlines out a nine-step process for calculating proposed monetary penalties, including a couple of novel elements.

The first step that the ICO will take is to carry out an assessment of the seriousness of an infringement, considering relevant factors under section 155 of the DPA. The factors replicate those of Article 83(2) of the GDPR, including the nature, gravity, and duration of the infringement, any action taken to mitigate the damage, the level of cooperation with the ICO, the categories of personal data, and previous data protection failures.

The second step is the assessment of the degree of culpability/fault of the organisation concerned. The ICO will determine this by assessing the technical and organisational measures and will also take into account the intentional or negligent character of the incident.

The third step is the determination of turnover. The ICO will review the relevant accounts and obtain expert financial, or accountancy advice if required, to determine the amount of turnover. In circumstances where

(Continued on page 17)

## CJEU rules that bulk data retention schemes are illegal

The Court of Justice of the EU has confirmed that national governments cannot force internet and phone companies to store information such as location data and metadata in the name of crime prevention or national security. This is a practice that is widespread among national security agencies in Europe.

The CJEU was giving judgment in favour of various rights advocacy organisations, including Privacy International and La Quadrature du Net, in relation to a number of cases that the organisations had brought against bulk data retention schemes run by UK, French and Belgian security and intelligence agencies.

According to the judgment, Member States may only authorise indiscriminate and bulk retention of data where they are faced with a serious threat to national security that proves to be genuine and present or foreseeable, subject to review by a court or independent body.

The judgment runs counter to certain elements of the UK's Investigatory Powers Act, as well as

(Continued on page 17)