

# Data Protection Ireland

Volume 12, Issue 3

May / June 2019

## Headlines

- New guidance on use of dash-cams, p.17
- Poland issues first GDPR fine, p.18
- DPC clarifies right to rectification complaints, p.20

## Contents

<i>Expert comment</i>	2
<i>Expanding the GDPR's journalism exemption — is all the world a stage?</i>	4
<i>'Sufficient guarantees' and technical due diligence when appointing processors</i>	7
<i>Anonymising personal data: where do we stand now?</i>	12
<i>Post GDPR enforcement in Germany — a sneak peek</i>	15
<i>News &amp; Views</i>	17

## DPC accused of 'blocking world on data privacy'

Brussels based *Politico Europe* has released a report — titled 'How one country blocks the world on data privacy' — questioning the Data Protection Commission's independence and willingness to apply the full force of the General Data Protection Regulation.

The 4,000 word report, the result of an investigation, claims that the GDPR's weakness is that companies are regulated by the Supervisory Authority where they're headquartered (i.e. have their controller) which

weakens the collective force of the EU to enforce the rules, leaving regulation up to smaller countries that could be more easily influenced instead. For big tech, this is usually Ireland, which —according to the report —"has a history of being overly accommodating to corporations (e.g. getting companies to set up shop in Ireland by promising little or no taxation)."

The report's authors state that Ireland has already shown it has a "laxer approach" to Facebook and other big tech companies

than Germany and France, and that big tech has had "easy access" to Irish politicians and government officials. It refers to the example of Facebook COO Sheryl Sandberg's reported involvement when the current Irish Data Protection Commissioner Helen Dixon was hired.

One of the experts quoted by *Politico*, Daragh O'Brien, stated that he did not completely agree with the editorial angle of the piece:

[\(Continued on page 17\)](#)

## DPC issues guidance on securing cloud-based environments

"Cloud-based environments offer many advantages to organisations. However, they also introduce a number of technical security risks which organisations should be aware of", warns the DPC in new guidance.

The guidance reminds organisations to determine and implement a documented policy and apply the appropriate technical security and organisational measures to secure

their cloud-based environments and protect from risks such as data breaches, hijacking of accounts and unauthorised access to personal data.

"Organisations should apply technical security and organisational security measures in a layered manner consisting of but not limited to: access controls; firewalls; antivirus; staff training; and policy development.

A layered approach to cloud-based security mitigates the risk of a single security measure failing which may result in a personal data breach," it states.

The guidance refers to cloud-based providers, such as Microsoft's Office 365 and Google's G-suite, as providing advanced settings and solutions which can assist

[\(Continued on page 17\)](#)