

Privacy & Data Protection

Volume 19, Issue 2

December 2018

Headlines

- Director liability for nuisance calls introduced in UK, p.18
- EU e-Privacy reforms hit stalemate, p.19
- Marriott data breach a Chinese effort?, p.20

Contents

<i>Expert comment</i>	2
<i>Data protection by Design and by Default: from theory to practice</i>	3
<i>Consent vs legitimate interest: Part 1</i>	7
<i>Reconciling innovation and regulation: mission impossible?</i>	10
<i>Dealing with Data Subject Requests – practical tips</i>	13
<i>News & Views</i>	17

UK government publishes plans for ‘no deal’ Brexit

The government has set out its intentions for ensuring the continuation of data protection law in the event of a no deal Brexit.

The government says that the GDPR will continue to apply under the EU Withdrawal Act (discussed on page 2), although it will remove references to ‘EU institutions and procedures’ and references to ‘Union or Member State law’.

The Information Commissioner’s Office will remain the independent data protection regulator. It will no longer be a member of

the European Data Protection Board, but the UK and EU have agreed to implement rules on co-operation between the ICO and the Board.

The UK will transitionally recognise all EEA states and Gibraltar as providing adequate protection for personal data. Personal data will continue to flow freely from the UK to these countries. However, this may be kept under review.

Organisations making data transfers from the EEA to the UK will need a transfer solution in place (Standard Contractual

Clauses or a viable alternative) to be clear that the UK is a data importer.

The UK will preserve the effect of the EU adequacy decisions on a transitional basis. Data transfers to these jurisdictions can continue uninterrupted. This covers: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and USA (under the Privacy Shield framework).

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

Irish regulator opens fresh GDPR investigation into Facebook

The Data Protection Commission in Ireland has commenced a GDPR investigation into Facebook on a broad spread of privacy issues. The opening of the investigation happened after Facebook disclosed a photo leak with compromised private images belonging to up to 6.8m users.

In mid December, the social network said that it had discovered a problem with the way hundreds of

third-party developers accessed photos using its app platform. The flaw leaked private photos that Facebook users had uploaded but not chosen to share publicly.

“Because of this bug, some third-party apps may have had access to a broader set of photos than usual for 12 days between September 13th to September 25th, 2018,” Facebook’s engineering director

Tomer Bar said. “Currently, we believe this may have affected up to 6.8m users and up to 1,500 apps built by 876 developers,” he added.

DPC Helen Dixon said in response to Facebook’s revelation that it had opened an investigation into the Silicon Valley company’s compliance with the EU’s General Data Protection Regula-

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