

# Privacy & Data Protection

Volume 16, Issue 3

January/February 2016

## Headlines

- EDPS begins year on intentional note p.18
- UK government announces new rules to crack down on nuisance calls, p.19
- Netherlands introduces new breach notification rules, p.20

## Contents

<i>Expert comment</i>	2
<i>EU General Data Protection Regulation: things you should know</i>	3
<i>The right to be forgotten — under spotlight</i>	6
<i>The Network and Information Security Directive — a practical perspective</i>	9
<i>Seven key data protection New Year's Resolutions companies should be making</i>	13
<i>Just how fair will processing notices need to be under the GDPR?</i>	16
<i>News &amp; Views</i>	18

## After four years of waiting, language of reform agreed

Agreement has finally been reached on the final text of the General Data Protection Regulation — four years after the first draft was released.

The Regulation is expected to be formally adopted in the next few weeks, and will come into effect two years later.

Among other things, the General Data Protection Regulation will involve much larger fines for breaches than under the existing rules — up to 20 million euros or 4% of a company's global turnover (1% lower than under earlier iterations of the new rules).

There will be a new obligation to appoint a Data Protection Officer for larger organisations, and more extensive rights for individuals, including the right to increased information on how data are processed (see the article on pages 16-17), and the rights to erasure and objection (pages 6-8).

The new GDPR will apply to data controllers *and* data processors (not just controllers as under the existing Directive). Companies established outside of the EU will also be covered if they offer services in the EU and are processing personal data of EU citizens.

In the UK, the Head of the data protection regulator Christopher Graham said that the ICO would be doing everything in its power to ease the introduction of the new rules — for data controllers and data subjects alike.

“Our approach to regulation begins with clear advice and guidance. We will focus on the new elements first, whilst remembering that there is much in the new regulation that will be familiar to us — the new principles are pretty much the same as the old ones”, he said.

[\(Continued on page 18\)](#)

## President signs federal Cybersecurity Information Sharing Act into law

President Barack Obama has signed into law the controversial Cybersecurity Information Sharing Act of 2015 (CISA) as part of a package of bills.

The Bill gives extensive new powers of monitoring by organisations and sharing between federal agencies of so called ‘threat data’.

In terms of the monitoring, the Bill authorises organi-

sations to monitor their information systems and all information stored on, processed by, or transiting the information system, as long as the monitoring is for the purpose of protecting the information or information systems.

Organisations are granted full immunity from government and private lawsuits and other claims that may arise out of

CISA-compliant monitoring in which they engage.

Companies may then share cyber threat information with seven specified federal agencies. These agencies include the Department of Defence (including the NSA) and the Office of the Director of National Intelligence, as well as the Department of Home-

[\(Continued on page 18\)](#)