Data Protection: What's Happening in 2017?

Laura Irvine, Associate and Solicitor Advocate

6 April 2017

Today we will cover …

- DP Basics
- Subject Access Requests and recent developments
- Compensation claims including *Woolley v Akram* and *Beyts v TIGLS*;
- Recent enforcement action from the ICO for data breaches
  - Charities, fundraising and fair processing;
  - Marketing; and
- GDPR Headline Changes (as we go)

The Data Protection Principles

1. Processing must be fair and lawful
2. Processing only for one or more specified purposes
3. Processing must be adequate, relevant and not excessive
4. Data accurate and up to date
5. Data not to be kept longer than necessary
6. Processing must be in accordance with data subjects' rights under the 1998 Act .
7. Adequate technical/organisational measures to protect data security
8. Transfers outside the EEA

“Data”

Information which is:

- being processed by equipment operating automatically in response to instructions
- recorded with the intention that it should be processed by means of such equipment,
- recorded in a **relevant** filing system
- recorded information held by a public authority

“Personal”

Information which is

- 'obviously about' a living individual; or

- clearly 'linked to' an individual because it is about his activities and is processed for the purpose of determining or influencing the way in which that person is treated.

So “Personal Data” is:

Data which relates to a living individual who can be identified or is identifiable –

- from that data, or
- from data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Includes expression of **opinion** about the individual.

“Processing”

- Storing
- Retrieving
- Accessing
- Modifying
- Deleting

Schedule 2
Main conditions for processing personal data

- You have consent from the individual
- The processing is necessary
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you.

Schedule 2
Main conditions for processing personal data

- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition.

“Sensitive Personal Data”

www.bto.co.uk

Sensitive Personal Data

a) racial or ethnic origin;
b) political opinions;
c) religious beliefs;
d) membership of a trade union;
e) physical or mental health or condition;
f) sex life;
g) the commission (or alleged commission) of an offence; or
h) any proceedings or disposal/sentence for any offence committed or alleged to have been committed.

NB: Financial information

Schedule 3
Main conditions for processing sensitive personal data

- You have explicit consent to the processing.
- The processing is necessary to comply with employment law.
- The processing is necessary to protect the vital interests of:
  - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
  - another person (in a case where the individual's consent has been unreasonably withheld).

Schedule 3
Main conditions for processing sensitive personal data

- Certain activities by charities
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.

Schedule 3
Main conditions for processing sensitive personal data

- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.
- The Data Protection (Processing of Sensitive Personal Data) Order 2000 - substantial public interest

Exemptions

1. National Security
2. Crime and taxation
3. Health, education and social work
4. Regulatory
5. Journalism, literature and art/what is in the public interest
6. Research
7. For legal proceedings or to obtain legal advice
8. Parliamentary privilege
9. Domestic purposes

Subject Access Requests

www.bto.co.uk

SARs: the basics

- Section 7 of the Data Protection Act 1998 (DPA) provides that a data subject is entitled to receive information constituting their personal data from anyone holding such data.
- Charge £10
- 40 calendar days within which to respond
- Solicitors can make requests on behalf of their clients

Main Exemptions

- Third party personal data
- Confidential references
- Publicly available information
- Crime and taxation
- Management information
- Negotiations with the requester
- Regulatory activity
- Legal advice and proceedings
- Social work records
- Separate consideration for health and educational records

What happens if you refuse to comply with a SAR?

- ICO powers
  - Correspondence
  - Enforcement Notice
- Court powers
  - Section 7(9) DPA
  - Case law
- Compensation
  - Section 13 DPA

Case law in summary – until recently!!

- SAR is only valid if made for one of the purposes set out in the Directive
- A SAR can be made for more than one reason
- Even if there is potential litigation in the background, a SAR may be valid if it is also for one of the purposes set out in the Directive
- A SAR should not be used *only* to circumvent proper court procedures

Dawson Damer v Taylor Wessing: Court of Appeal

- Collateral Purpose
- Legal Professional Privilege

Holyoake v Candy

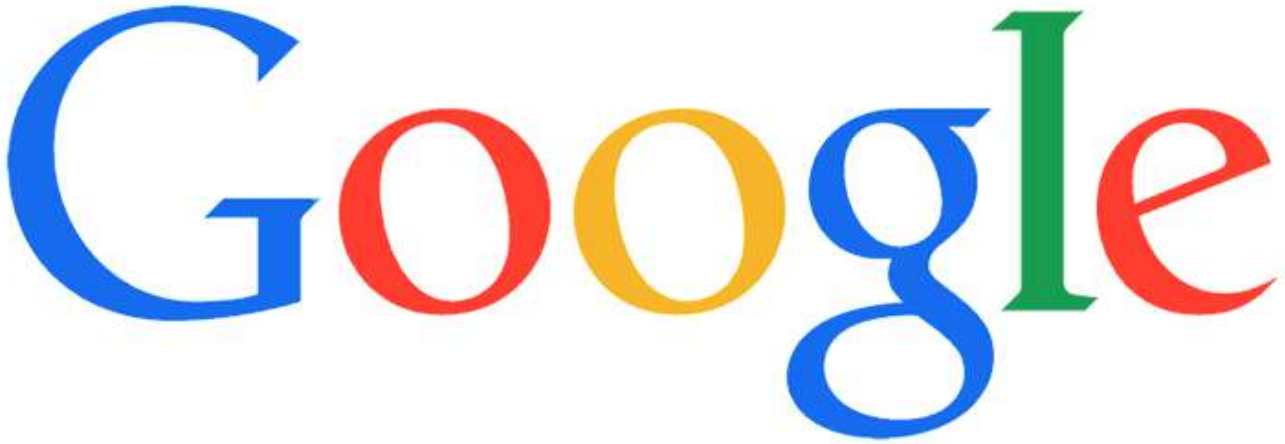
- Improper motive?
- Must be a strong reason to remove the LPP exemption

Ittihadieh v RTM Co Ltd
Deer v University of Oxford
University of Oxford v Deer

- SAR Limitation - Domestic processing
- Processing for personal and household affairs

Compensation claims: section 13 DPA

Vidal-Hall v Google



Woolley v Akram

Beyts v TIGLS

ICO Fines

www.bto.co.uk

Section 55A DPA: Monetery Penalty Notices

- Serious breach
- Of a kind likely to result in substantial damage or substantial distress
- Deliberate or the Data Controller should have known that there was a risk of the breach
- And that the Data Controller failed to take reasonable steps to prevent the breach
- Fines of up to £500,000

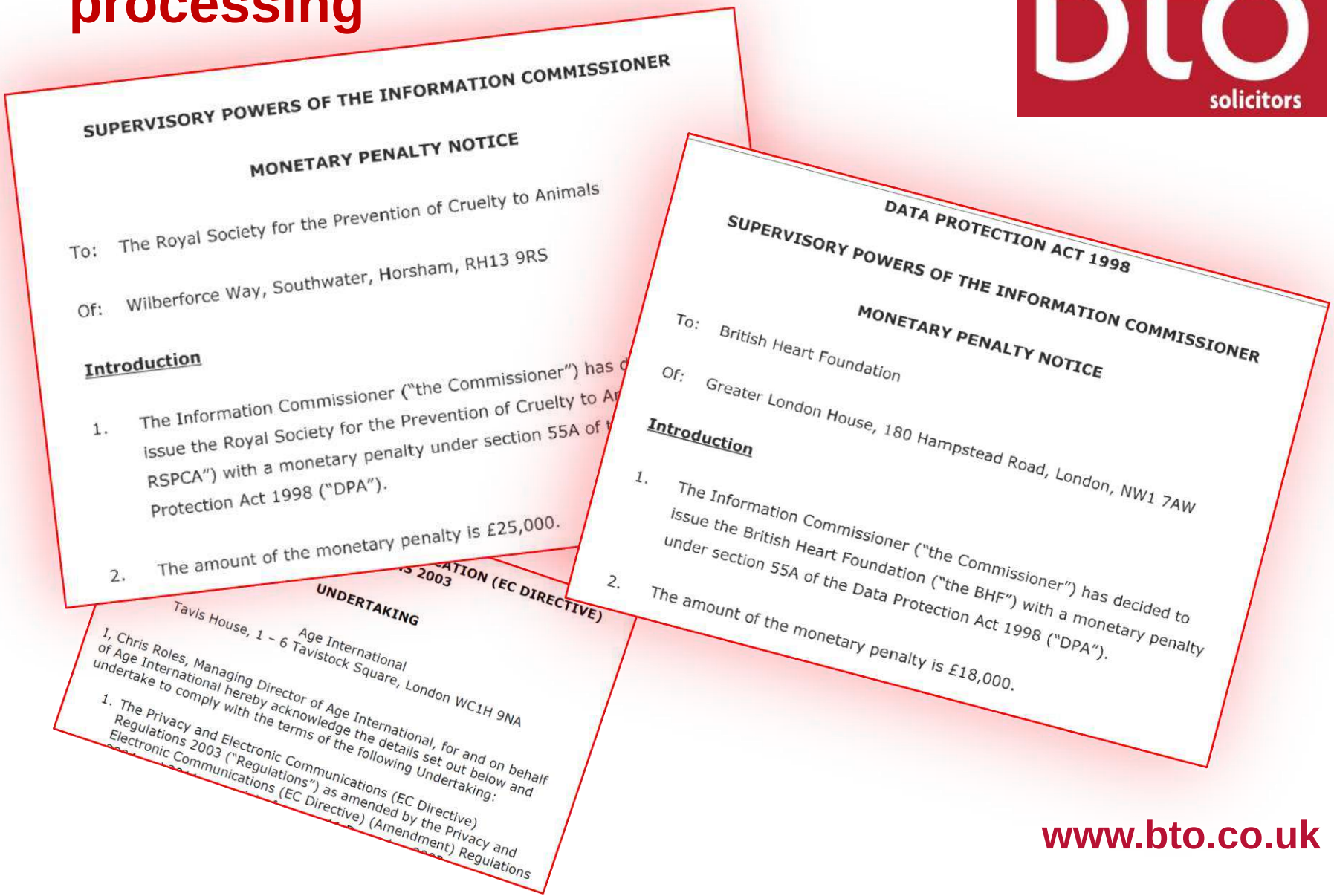
Common Breaches

- Loss of paperwork
- Faxes and emails to the wrong place
- Unencrypted end user devices
- Cyber attacks

- All breaches of the 7th Principle

- All sectors: public, private and third

Charities, fundraising and fair processing



SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: The Royal Society for the Prevention of Cruelty to Animals

Of: Wilberforce Way, Southwater, Horsham, RH13 9RS

Introduction

1. The Information Commissioner ("the Commissioner") has d
issue the Royal Society for the Prevention of Cruelty to An
RSPCA") with a monetary penalty under section 55A of t
Protection Act 1998 ("DPA").

2. The amount of the monetary penalty is £25,000.

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: British Heart Foundation

Of: Greater London House, 180 Hampstead Road, London, NW1 7AW

Introduction

1. The Information Commissioner ("the Commissioner") has decided to issue the British Heart Foundation ("the BHF") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA").

2. The amount of the monetary penalty is £18,000.

...ATION (EC DIRECTIVE)
...S 2003

UNDERTAKING

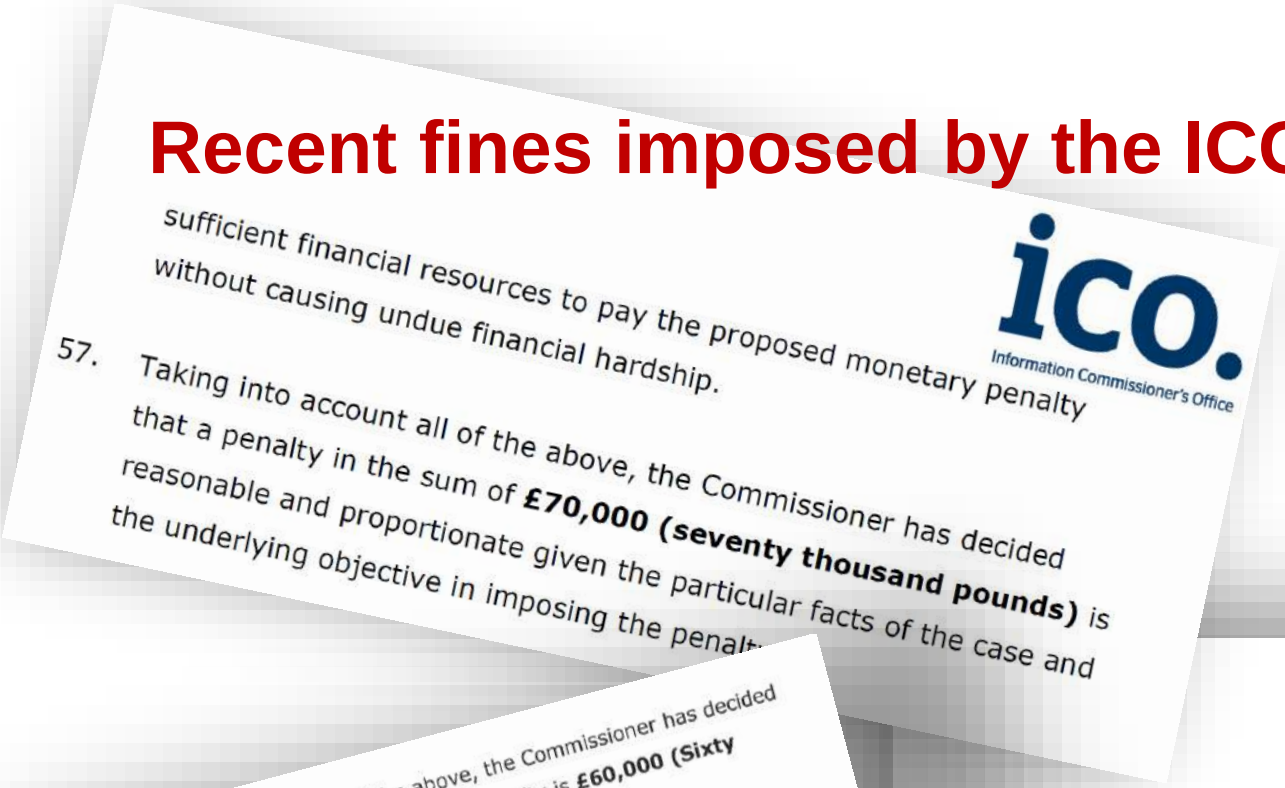
Age International
Tavis House, 1 - 6 Tavistock Square, London WC1H 9NA

I, Chris Roles, Managing Director of Age International, for and on behalf of Age International hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

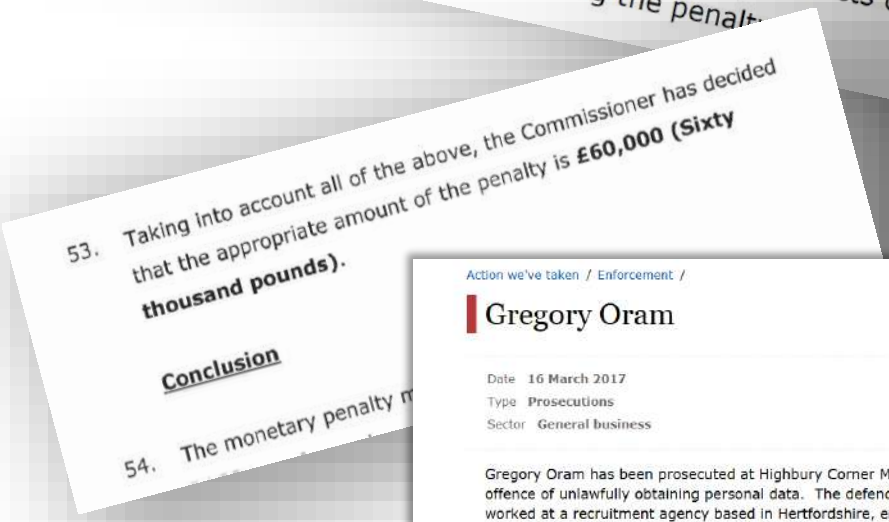
1. The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("Regulations") as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations

www.bto.co.uk

Recent fines imposed by the ICO;


sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship.

57. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£70,000 (seventy thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalt


53. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£60,000 (Sixty thousand pounds)**.

Conclusion

54. The monetary penalty n

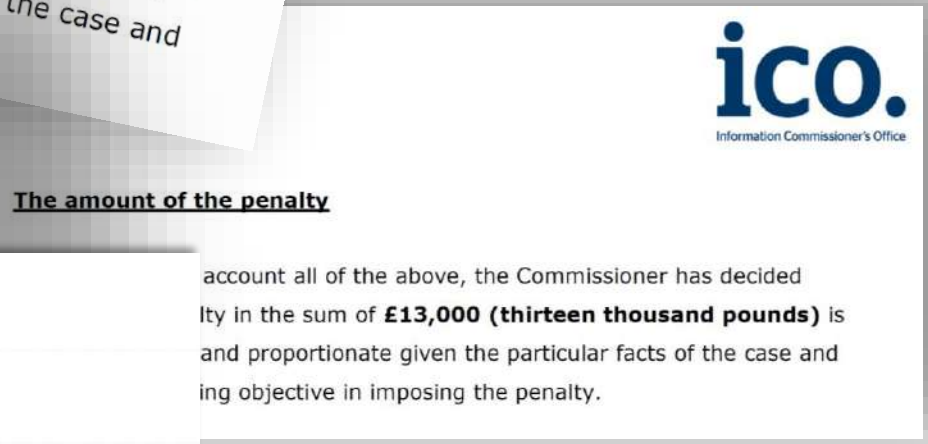

Action we've taken / Enforcement /

Gregory Oram

Date 16 March 2017
Type Prosecutions
Sector General business

Gregory Oram has been prosecuted at Highbury Corner Magistrates' Court for an offence of unlawfully obtaining personal data. The defendant, who at the time worked at a recruitment agency based in Hertfordshire, emailed the personal data of approximately 500 candidates to his personal email address as he was leaving to start a new rival recruitment company. The data included contact details, candidate files, consisting of identification and qualification documents, references, DBS checks, as well as a large number of CVs. Mr Oram took the data to use as potential clients for his new business.

Mr Oram pleaded guilty to the offence under section 55 of the Data Protection Act, and was fined £170, ordered to pay £360 prosecution costs and a £30 victim surcharge.


The amount of the penalty

account all of the above, the Commissioner has decided
lty in the sum of **£13,000 (thirteen thousand pounds)** is
and proportionate given the particular facts of the case and
ing objective in imposing the penalty.

www.bto.co.uk

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

ico.
Information Commissioner's Office

ico.org.uk

In Conclusion: where are we with GDPR Guidance?

- ICO Guidance on Data Protection Reform: 12 Steps; Overview Document; Privacy Notices CoP and Consent Consultation document
- Art 29 WP Guidance: on DPOs; Data Portability and Supervisory Authorities
- For 2017 Art 29 WP Guidance: certification; high risk processing; DPIA, administrative fines, the EDPB; consent; profiling; transparency; data transfers to third countries; data breach notifications

Data Protection: What's Happening in 2017?

Laura Irvine, Associate and Solicitor Advocate

6 April 2017