# The New General Data Protection Regulation

Presented by:

**Ibrahim Hasan**

**ACT NOW TRAINING** Anchor House, Thornhill Road, Dewsbury, WF12 9QE

**TEL** 01924 451054 **FAX** 01924 451129 **WEB** www.actnow.org.uk **EMAIL** info@actnow.org.uk

# CONTENTS



## PLEASE NOTE

Data Protection and related legislation is a very complex subject. The contents of this seminar and documentation are meant for you to consider on the basis of general discussion. It is not advice or opinion (legal or otherwise). You should obtain expert legal advice on your specific issues from a qualified solicitor.
Any liability (in negligence or otherwise) arising from you acting or refraining to act as a result of anything in this seminar or documentation is excluded.

## COPYRIGHT NOTICE

# Speaker Biography

## Ibrahim Hasan – Solicitor

Ibrahim Hasan is a recognised expert on data protection, freedom of information and surveillance law. He was previously Principal Solicitor at Calderdale Council and has worked for Bradford Council and Nottinghamshire County Council. He has also held positions as an associate with the Institute of Public Finance and as a non executive director of an NHS Trust. Ibrahim is now a full time trainer and writer on information law issues.

Ibrahim is very much in demand as a presenter at courses and conferences throughout the UK. He has conducted training sessions for many national organisations as well as local authorities and the NHS. His high profile clients include the Olympic Delivery Authority, the House of Commons, the Scottish Executive, General Medical Council, the Independent Police Complaints Commission, Birmingham City Council and various other local and central government organisations. Ibrahim's expertise has also taken him to China, Malta and Ghana. In January 2015 he travelled to Brunei to train government officials in conducting data protection audits.

Ibrahim's articles have appeared in many professional journals including the Local Government Chronicle, Benefits Magazine, IRRV Insight Magazine and Solicitors Journal. He is a member of the European Information Managers Group (EURIM) and has contributed to the privacy law aspects of a book entitled "Spy TV – Just who is the digital revolution overthrowing?" which won a Big Brother Award from Privacy International.

Ibrahim currently writes the Freedom of Information Update column in the Law Society Gazette and is a guest lecturer on the University of Northumbria's LLM in Information Rights Law. He was recently made an Honorary Fellow of the Information and Records Management Society.

Ibrahim is often interviewed in the local and national media as a legal expert. He has appeared on the "Today program" on Radio 4 as well as "McIntyre Investigates" on Radio 5.

**Contact Details:**

Tel: 01924 451054

Email : info@actnow.org.uk

# Data Protection Quiz

***Decide which of the following statements are true and which are false.***

1. The Data Protection Act 1998 (DPA) came into force on 2nd March 2000.

2. The following is all personal data under the DPA: personnel records, mailing lists, e mail addresses, interview notes and the name of the director of a company.

3. There are 8 Data Protection Principles under the DPA that have to be complied with.

4. Breach of the DPA could lead to a fine of up to £50,000.

5. A Data Subject can sue a Data Controller if he/she has suffered damage as a result of a breach of the DPA.

6. The only schools that the DPA applies to are voluntary aided schools and academies.

7. All Data Controllers have to go through the process of Notification. There are no exceptions.

8. Recklessly disclosing personal data carries a term of imprisonment of up to two years.

9. DPA Subject Access Requests must be answered within 40 calendar days.

10. Legal advice is exempt from the right of Subject Access.

11. The maximum that can be charged for a Subject Access Request is £10 plus photocopying expenses.

12. The Information Commissioner has the power to enter and search premises and seize documents.

13. If the police ask to see personal data held by an employer about employees, it must always be disclosed.

14. Parents always have a right to see their child's personal data.

15. If a company sends direct marketing mailshots to former clients after having sought their consent, those clients still have a right to object to that marketing in the future.

16. Signs should be installed wherever CCTV cameras are in operation.

17. The new EU General Data Protection Regulation (GDPR) will completely replace the Data Protection Act 1998.

18. Under the new GDPR, breaches of data security will have to be notified to the Information Commissioner no later than 24 hours from the time of the breach.

19. The maximum fine for a breach of the GDPR will be 4% of annual turnover or 20 million Euros.

20. Now that the UK has voted for Brexit we do not need to worry about the GDPR.

# The General Data Protection Regulation 2016 (GDPR)

Ibrahim Hasan
Solicitor
*Act Now Training*

## GDPR After Brexit ?

**GDPR**
Published 4th May 2016

In force 25th May 2018
Great Repeal Bill

**Article 50**

If triggered March 2017

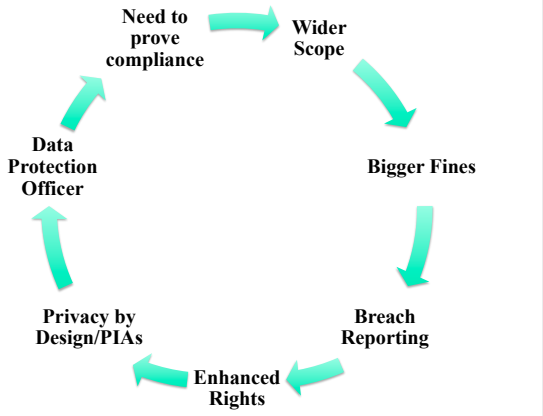
2 years

EU Exit March 2019

## No Big Changes

- Definition of personal data
- The DP Principles
- Existing data subject rights
- Exemptions (delegated)
- Information Commissioner

## What's New?




## Fines under GDPR

- €10,000,000 or 2% of turnover
- €20,000,000 or 4% of turnover

## ICO Powers


## Criminal Offences

- Failure to notify or to notify changes
- Failure to comply with written request
- Failure to comply with a Notice
- Unauthorised obtaining/disclosing
- Procuring a disclosure to another person
- Unlawful selling
- Enforced Subject Access

THE COURIER.co.uk

Taking you to the heart of Tayside and Fife

News Sport Community Living Opinion Photos Beezer Deals Family announcem

You are here: Home > News > Perthshire

### Police officer fined for data protection offences

A police officer from Perthshire has been fined after breaking data protection laws involving several women.

Gordon Isdale (31), of Blackford, is understood to have resigned from Central Scotland Police following a range of offences committed at Larbert Police Station, Stirlingshire, between 2007 and 2010.

Published in the Courier : 12.11.12
Published online : 12.11.12 @ 09.46am

SHARE Send link

Last week, Isdale was fined £1,600 at Stirling Sheriff Court after he admitted breaching the Data Protection Act. One of the charges related to the use of a confidential system to access information on individuals.

PC Isdale targeted several women, including transsexual Leeze Lawrence, to whom he sent text and phone messages.

A probe was subsequently launched by Central Scotland Police and officers found Isdale had used their computer system to access information on women.

It is understood he looked into the background of around 130 people during a three-year period while working as a policeman at Larbert Police Station.

Stirling Sheriff Court heard last week how he used three different computer systems to carry out searches on one woman over 12 months between 2009 and 2010.

The court heard how Isdale pleaded guilty to eight offences of breaching the Data Protection Act between November 2007 and August 2010.

## Man's £18k payout after ex-girlfriend viewed his medical records

Plymouth Herald Follow Saturday, January 28, 2012

A MAN has won £18,000 damages after his ex-girlfriend probed his medical records while working at Derriford Hospital.

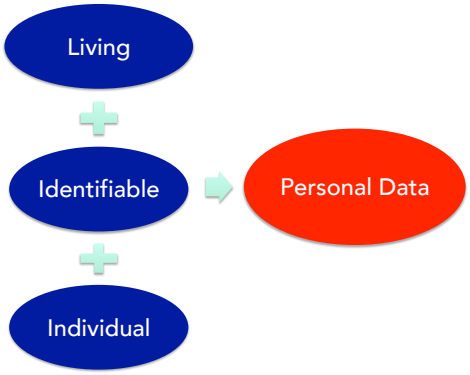
Plymouth Hospitals NHS Trust was ordered to pay the sum to Sean Grinyer, aged 33, of Crownhill, at a county court civil hearing.

Do you process personal data?

YES

**ACT APPLIES TO YOU**

**Notification** | **8 Principles** | **Individual Rights**



Do you process personal data?

YES

ACT APPLIES TO YOU

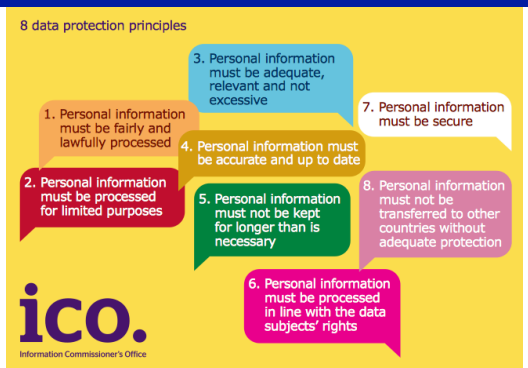
Notification | 8 Principles | Individual Rights

## Record Keeping (Art 24)

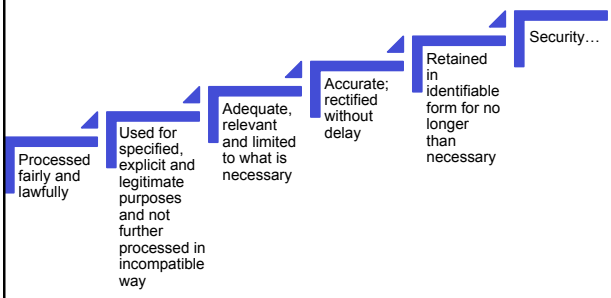
- Name of controller/joint controller/DP Officer
- Purpose of processing
- Categories of data subject/personal data
- Recipients
- Use of profiling
- International Transfers
- Time limits for erasure
- Legal Basis
- Security measures

Available to the ICO on request

## The Data Protection Principles



## 6 GDPR Principles




## First Principle

Personal data shall be processed fairly and lawfully

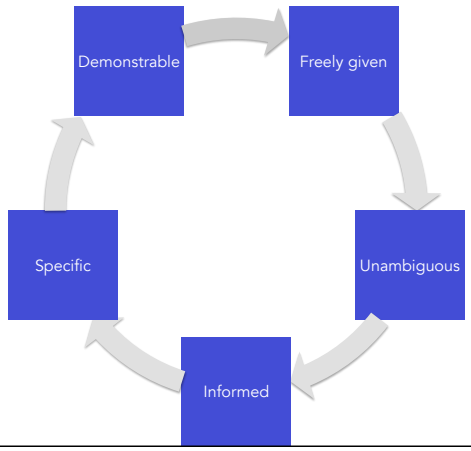
- Schedule 2
- Schedule 3

## Schedule 2 Conditions

Consent
Contractual purposes
Legal obligation
Protect vital interests
Public functions – justice, public duty etc
Legitimate interests

## Consent under GDPR - Art 4

"…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."




## Sensitive Personal Data

- Racial/ethnic origin
- Sexual life
- Political opinions
- Religious beliefs
- Physical/mental health
- Trade union membership
- Alleged/actual criminal record

## Schedule 3 Conditions

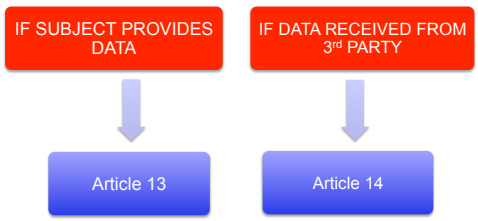
- Explicit consent
- Employment rights/obligations
- Vital interests
- Legitimate club use
- In public domain
- Public functions
- Legal proceedings/advice
- Medical purposes
- Equality Monitoring

## Fair Processing Code

The data controller should ensure that the data subject is provided with at least -

- the identity of the data controller & representative
- the purpose(s) for which data are to be processed
- any further information necessary

## GDPR Privacy Notices



## Contents

- ID of Data Controller
- Contact details of DPO
- Purpose of processing and legal basis
- Legitimate Interests
- Recipients
- Data Transfers

## Contents (2)

- Retention
- Individuals' rights
- Right to complain to ICO
- Consequences of not providing data (statutory/contractual requirement)
- Automated Decisions
- Sources (incl. public sources)

## The Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

## The Third Principle

Personal data shall be adequate, relevant and not excessive

## The Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

## The Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

## The Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

## The Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

### Key data security issues for each sector in Q1 2015/16

The main data security issues within the **health** sector are:

- Loss/theft of paperwork – 33% of health related incidents.
- Data being posted/faxed to incorrect recipient – 26% of incidents.

The main issue for **local government** is data being posted/faxed to the incorrect recipient – 36%.

The main issue for **general business** is insecure web pages (including hacking incidents) – 25%.

The main issue within the **education** sector is loss or theft of unencrypted devices – 26%.

The main issues within the **finance, insurance and credit** sector are:

- Data being posted or faxed to the incorrect recipient – 33%.
- Loss/theft of paperwork – 22%.

The main issue within the **charities and voluntary** sector is loss or theft of paperwork – 27%.

## Contracts With Data Processors

- Made or evidenced in writing
- Processor to act only on Controller's instructions
- Mirror Controller's obligations
  - » Security
  - » Employees

## Joint Working

Ealing
www.ealing.gov.uk

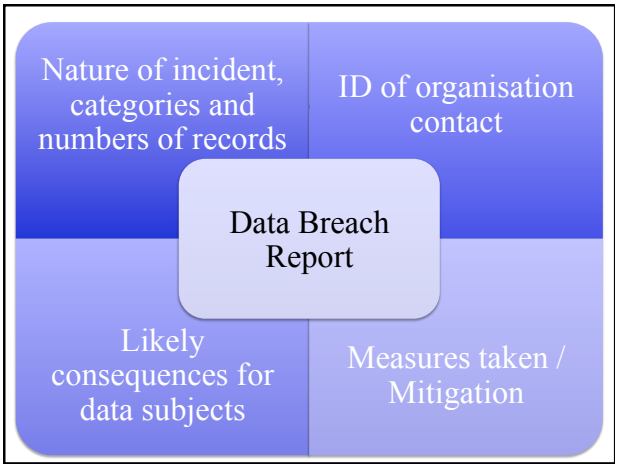
London Borough of Hounslow

£80,000
unencrypted laptop

£70,000
no contract - no monitoring

## Breach Reports (Art 33/34)

Normally report to ICO within 72 hours → If HIGH RISK then report to data subjects without undue delay → Exceptions apply




## Individual Rights

1. Subject Access
2. Prevent Processing
3. Direct Marketing
4. Automated Decisions
5. Compensation/Rectification

Court may order Compliance

## GDPR Subject Access (Art 15)

## The General Rules

- 1st Principle
  - Individual should be given FPC Information
  - Data should only be used for specified purposes
  - Consent must be obtained for ancillary purposes
  - Data should not be disclosed without consent
- Subject Access
  - Individuals must be given access to all their personal data

## Exemptions

S. 28 - National security

S. 29 - Crime and taxation

S. 30 - Health, education & social work

S. 31 - Regulatory activity

S. 32 - Journalism, literature & art

## Exemptions

S. 28 - National security

S. 29 - Crime and taxation

S. 30 - Health, education & social work

S. 31 - Regulatory activity

S. 32 - Journalism, literature & art

## Exemptions (2)

S. 33 - Research, history & statistics

S. 34 - Publicly available by any enactment

S. 35 - Required by law/proceedings

S. 36 - Domestic purposes

## Miscellaneous Exemptions

References

Management forecasts

Corporate finance

Negotiations

Exam marks/scripts

Legal privilege

Self incrimination

## Right To Be Forgotten - Art 17

Must delete if:

– no longer required

– consent withdrawn and no overriding legitimate grounds for processing

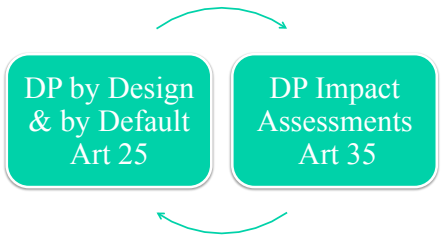
Exemptions apply

## Data Portability - Art 20

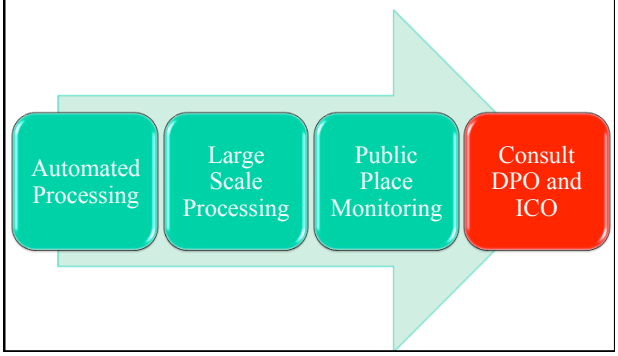
- Right to receive data in a structured, commonly used machine readable format where originally processed through consent or contract and processing is automated
- Can have it directly transmitted to another data controller
- Exceptions apply

## Additional GDPR Requirements

## Practical Skills



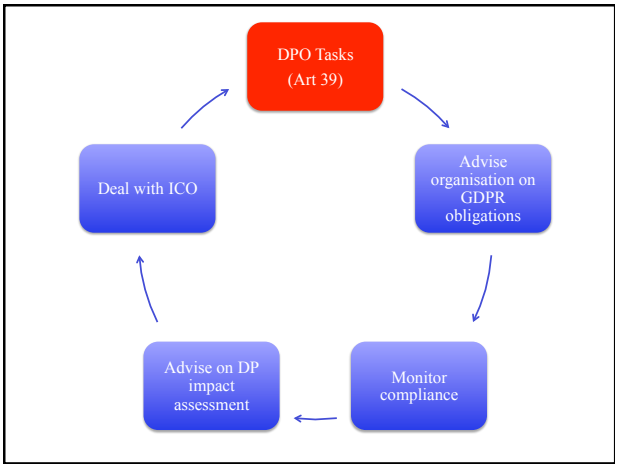
## High Risk




## The DPO - Who Needs One?

- Public Authorities
- DC's core activities include "regular and systematic monitoring of data subjects on a large scale"
- DC conducts large-scale processing of "special categories of personal data"

## The DPO - Art 37




## DPA/GDPR Action Plan

Accountability - DP Audit

Consent and Control - Privacy policies

Breach Management - Security/breach policies

Staffing - DPO and training


**Practical**

**No Rote Learning**

**Short Exam**

**Open Book Project**

**Covers GDPR**

**Syllabus Endorsed by UoW**

## Advice Helplines

1. Data Protection
2. Freedom of Information and EIR
3. RIPA/RIPSA and Surveillance Law

Annual subscription per organisation

## Getting in Touch

info@actnow.org.uk

01924 451054

@ActNowTraining

# The New EU General Data Protection Regulation (GDPR)

The clock has started on the biggest change to the European data protection regime in 20 years. After four years of negotiation, the new EU General Data Protection Regulation (GDPR) has now been formally adopted by the European Parliament. It will take effect twenty days from its post-vote publication in the Official Journal (May 2018) giving Data Controllers two years to prepare.

The Regulation will directly replace member states' own data protection legislation (the Data Protection Act 1998 (DPA) in the UK). It will apply to any entity offering goods or services (regardless of payment being taken) and any entity monitoring the behaviours of citizens residing within the EU. Companies are now directly responsible for DP compliance wherever they are based (and not just their EU based offices) as long as they are processing EU citizens' personal data.

**Principles**

The Data Protection Principles, as set out in the DPA, remain but they have been condensed into six as opposed to eight principles. Article 5 of the Regulation states that personal data shall be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Consent**

Like the DPA, the Regulation will require Data Controllers to have a legitimate reason for processing personal data. If they rely on the consent of the Data Subject, they must be able to demonstrate that it was freely given, specific, informed and unambiguous for each purpose for which the data is being processed. Consent can be given by a written, including electronic, or oral statement. This could include the Data Subject ticking a box when visiting a website, choosing technical settings for social network accounts or by any other statement or conduct which clearly indicates his/her acceptance of the proposed processing of personal data. Silence, pre-ticked boxes or inactivity will no longer constitute consent.

**Children**

The Preamble to the Regulation states:

> *"Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child."*

Article 8 requires that where the personal data of a child under 16 is being processed to provide "information society services" (e.g. online businesses, social networking sites etc.) consent must be obtained from the holder of parental responsibility for the child. Member states are allowed though to lower this threshold where appropriate but not below the age of 13.

**Data Subjects' Rights**

The list of rights that a Data Subject can exercise has been widened by Section 2 of the Regulation. The subject access right, rectification and being able to object to direct marketing remain. The right to have personal data processed for restricted purposes and the right to transfer data/have it transferred to another Data Controller (data portability) are new rights.

In addition Article 17 introduces a "Right To Be Forgotten" which means that Data Subjects will be able to request that their personal data is erased by the Data Controller and no longer processed. This will be where the data is no longer necessary in relation to the

purposes for which it is processed, where Data Subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with the Regulation. However, the further retention of such data will be lawful in some cases e.g. amongst others, where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims.

To strengthen the "Right To Be Forgotten" in the online environment, the Regulation requires that a Data Controller who has made the personal data public should inform other Data Controllers which are processing the data to erase any links to, or copies or replications of that data.

**Data Protection by Design**

Data Controllers will be expected to include data protection controls at the design stage of new projects involving the processing of personal data. Where they wish to process personal data that poses potentially high risks they will have to, prior to the processing, carry out a Data Protection Impact Assessment. Supervisory Authorities (the member state's DP regulators e.g. the Information Commissioner's Office (ICO) in the UK) will be able to produce lists as to what sort of processing would warrant such an assessment.

**Notification**

The current system of Notification under the DPA will be replaced by a requirement for Data Controllers to keep an internal record in relation to all personal data they process (Article 30). The record must include, amongst other things, details of the purpose of processing of personal data, recipients, transfers to third countries, time limits for erasure as well as a general description of the technical and organisational measures in place protecting the data.

**Data Breaches**

Currently in the UK there is no legal obligation, under the Data Protection Act 1998 (DPA) to report personal data breaches to anyone. However the Information Commissioner's Office (ICO) guidance recommends that serious breaches should be brought to its attention. Last year telecoms company Talk Talk was the subject of a cyber attack in which almost 157,000 customers' personal details were hacked. The company was criticised for its slow response especially the time it took to inform the ICO and customers.

The Regulation contains a new obligation on Data Controllers to repot data breaches. Article 4 of the Regulation defines a personal data breach as:

> *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*

Article 33 of the Regulation requires that, as soon as the Data Controller becomes aware that a personal data breach has occurred, it should without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO, unless the controller is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification to the ICO and information may be provided in phases without undue further delay.

Furthermore Data Subjects should be notified without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms, in order to allow them to take the necessary precautions. This notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. This should be done as soon as reasonably feasible, and in close cooperation with the ICO and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities).

**Fines**

Currently the ICO can issue a Monetary Penalty Notice of up to £500,000 for serious breaches of the DPA. The Regulation introduces much higher fines.

For some breaches of the Regulation (e.g. failing to comply with Data Subjects' rights or the conditions for processing) Data Controllers can receive a fine of up to 4% of global annual turnover for the preceding year (for undertakings) or 20 million Euros. For other breaches (e.g. failing to keep records or complying with security obligations) the fine can be up to 10 million Euros or 2% of global annual turnover (for undertakings).

**Compensation**

The Regulation also contains a right to civil damages just like under S.13 of the DPA. Article 82 of the Regulation states:

> *"Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."*

This may see more in Data Subjects taking legal action against Data Controllers for data breaches. There may even be more class actions like the one against the London Borough of Islington in 2013 when 14 individuals settled for £43,000 in compensation after their personal data was disclosed without their authority. This action followed an ICO investigation, which resulted in the council being fined £70,000 under the DPA.

**Data Protection Officer**

Section 4 of the Regulation introduces a statutory role of Data Protection Officer (DPO). Most organisations handling personal data, both Data Controllers and Data Processors, will require a DPO who will have a key role in ensuring compliance with the Regulation. A group of undertakings may appoint a single DPO provided that he/she is easily accessible. Public bodies may also have a single DPO for several such authorities or bodies, taking account of their organisational structure and size.

The DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39. These are:

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation, including the assignment of responsibilities, awareness- raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO);

- to act as the contact point for the supervisory authority on issues related to the processing of personal data

The Regulation is accompanied by the EU Policing and Criminal Justice Data Protection Directive which contains new rules for Data Protection when applied to crime and justice, but which can be implemented by each Member State through its own laws with greater flexibility.

There is a lot to learn and do in the next two years. All Data Protection practitioners and lawyers need to read the Regulation and consider its impact on their organisation and clients. Training and awareness at all levels needs to start now.

***Ibrahim Hasan is a solicitor and director of Act Now Training (www.actnow.org.uk).***

# Data Protection Resources

www.actnow.org.uk
Articles and webcasts of data protection and data sharing

https://actnowtraining.wordpress.com/
Our blog on all things DP, GDPR, FOI and RIPA

www.ico.org.uk
Information Commissioner's website

https://ico.org.uk/for-organisations/data-protection-reform/
ICO's GDPR microsite

http://www.twobirds.com/en/hot-topics/general-data-protection-regulation
Bird and Bird GDPR Guide

http://tinyurl.com/ozwbg6e
ICO Outsourcing Guide

http://tinyurl.com/oaymshj
Model Data Processing Contract

http://tinyurl.com/p88z4m4
Sample DP clauses

http://tinyurl.com/phf8rsy
Model clauses for transferring data to third countries

https://www.jiscmail.ac.uk/cgi-bin/webadmin?A0=DATA-PROTECTION
Jiscmail DP Forum

https://panopticonblog.com/
Great information law blog from 11KBW

www.informationlaw.org.uk
Articles on information/surveillance law by Ibrahim Hasan

| | Action/To Do | Who/When |
|---|---|---|
| **1** | | |
| **2** | | |
| **3** | | |
| **4** | | |
| **5** | | |
| **6** | | |
| **7** | | |
| **8** | | |
| **9** | | |
| **10** | | |