



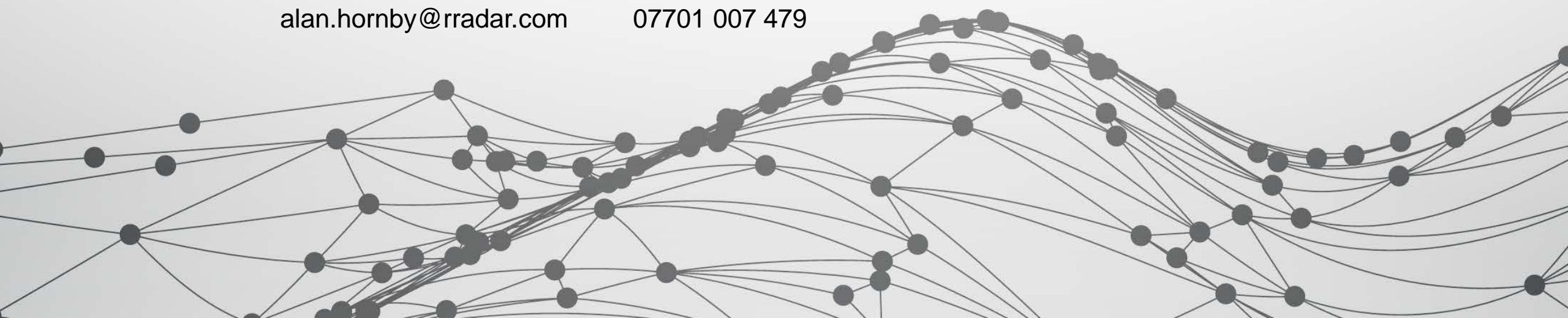
# GDPR

## General Data Protection Regulation

**Alan Hornby ACII**  
CII Accredited Advanced Trainer

alan.hornby@rradar.com

07701 007 479



# Objectives

- Explain the main aspects of GDPR
- List the changes organisations will need to consider
- Explain why you have to comply with the GDPR and what might happen if you don't.
- Outline the steps you can take to prepare for GDPR compliance.
- Discuss the impact of GDPR on the insurance profession

# What is the GDPR?

- GDPR replaces Data Protection Act 1998
- Direct effect on 25 May 2018 – no need for UK legislation
- Brexit will not effect GDPR – UK must have similar data management standards

- Stronger rights for consumers
- Data - Boardroom issue
- Evolution not revolution



## Data Protection Act 1998







# Accountability Principle

The 'Accountability Principle' (Article 5(2))  
Previously implicit under DPA, now explicit :

'controllers shall be responsible for, **and be able to demonstrate compliance with** the principles.'

Must implement technical and organisational measures to demonstrate compliance such as :

- Data protection policies
- Training
- Internal audits
- Data Protection Officers (where appropriate)
- Adopting privacy by design
- Data protection impact assessments (where appropriate)

(NB Code of Practice)

# Scope

- Applies to controllers and processors
- Definition of data – broader
- Includes IP address

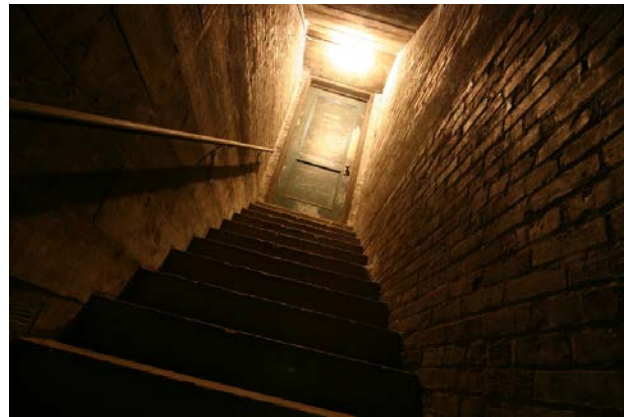




# Special category of data

- Racial or ethnic origin
- Political opinions or philosophical beliefs
- Trade union membership
- Processing of genetic data
- Biometric data (for purpose of uniquely identifying a natural person)
- Health
- Sex life or sexual orientation

# Where is data stored ?





# Consent

- Clear and affirmative
- Easy to distinguish – verifiable
  - Keep records
- Right to withdraw
  - Easy

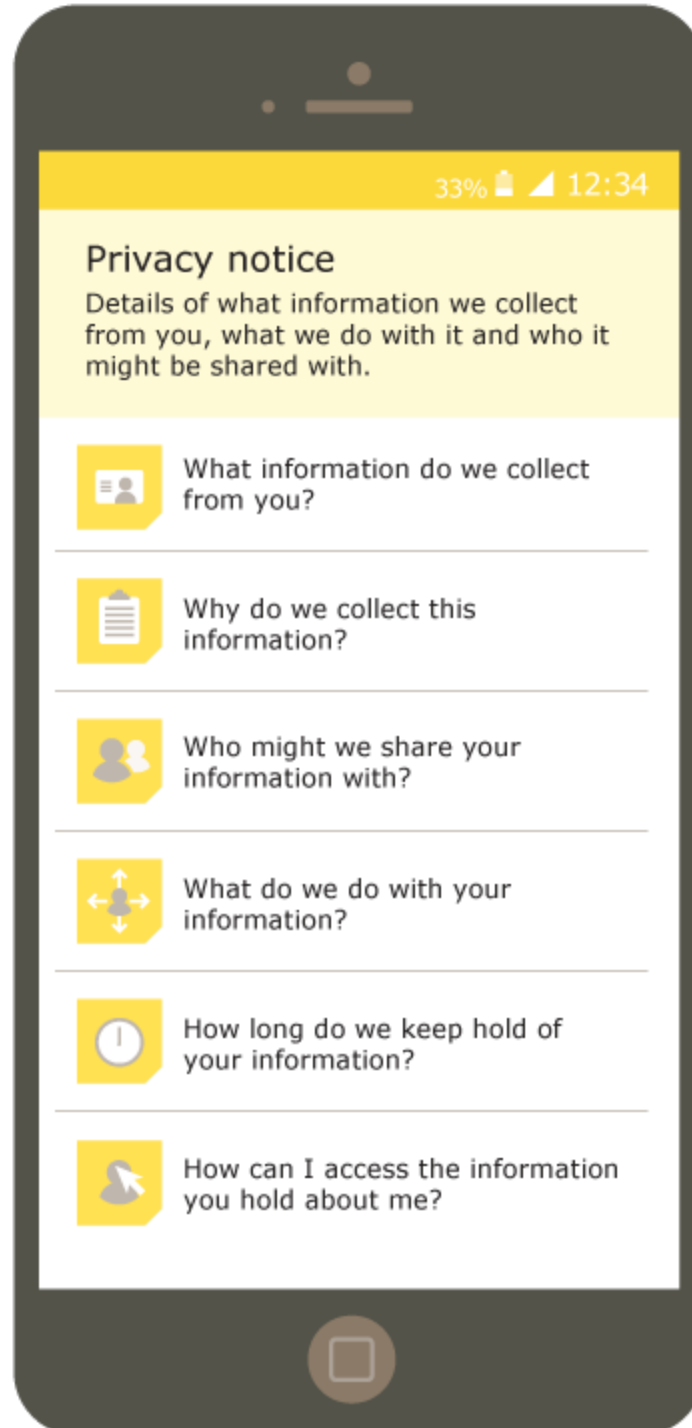




# Lawfulness of processing conditions

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

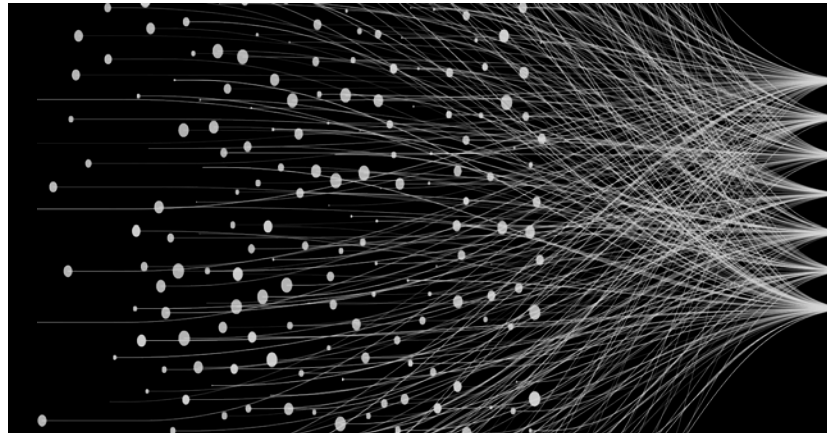






# Rights

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling



# Erasure

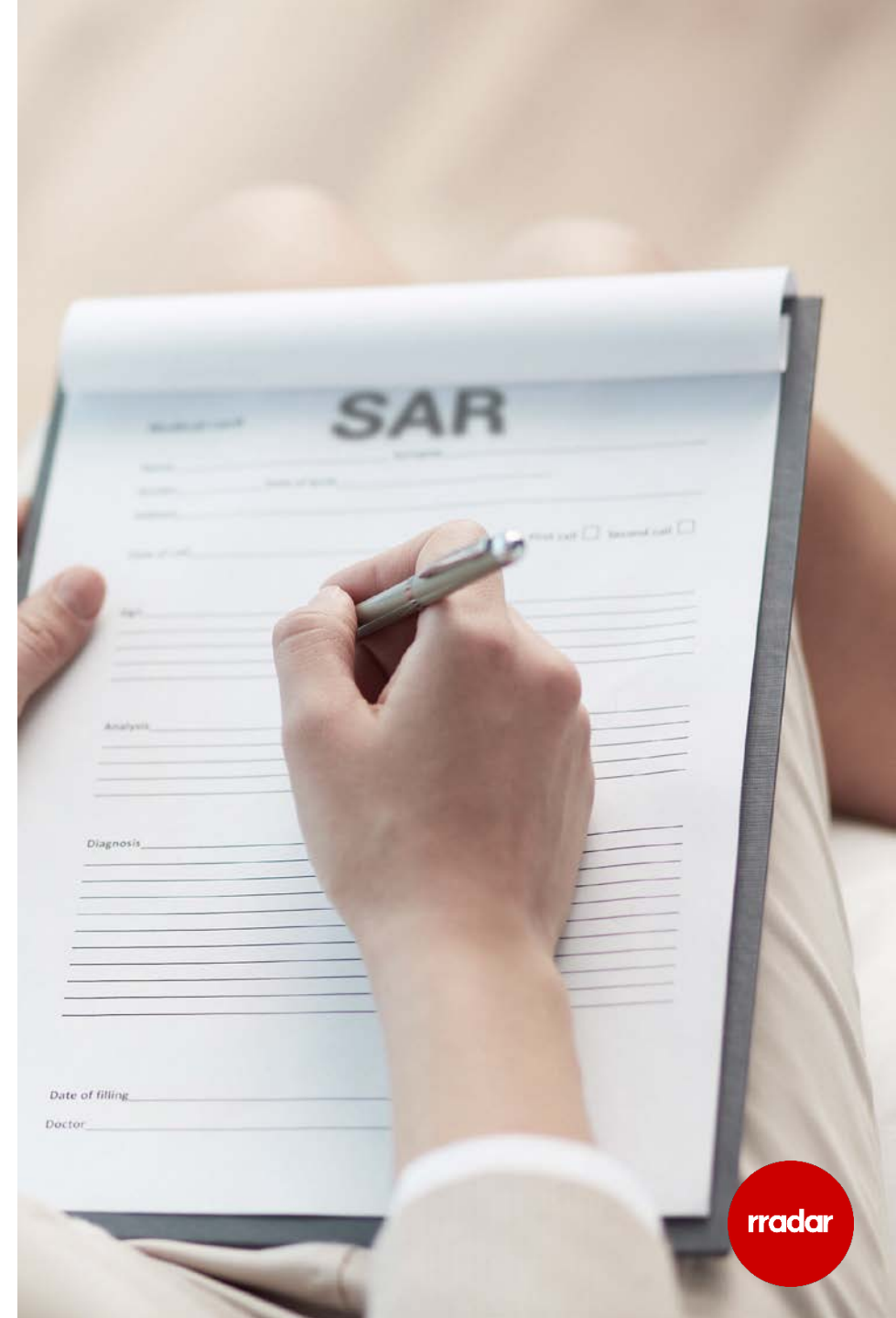
If data is shared – inform other organisations without delay

delete



# Subject Access Request (SAR)

- Reduced timescales – 1 month
- Provide free of charge





# Portability

- Obtain and reuse



# What does all this mean?

- Firms required demonstrate compliance
- MUST provide evidence
- Implement technical and organisation measure
- ICO recommends data protection impact assessment
- Freely available on ICO website

# Data Protection Officer

- Public authorities
- Systematic monitoring
- Large scale process of special category of data
- Health, life insurance

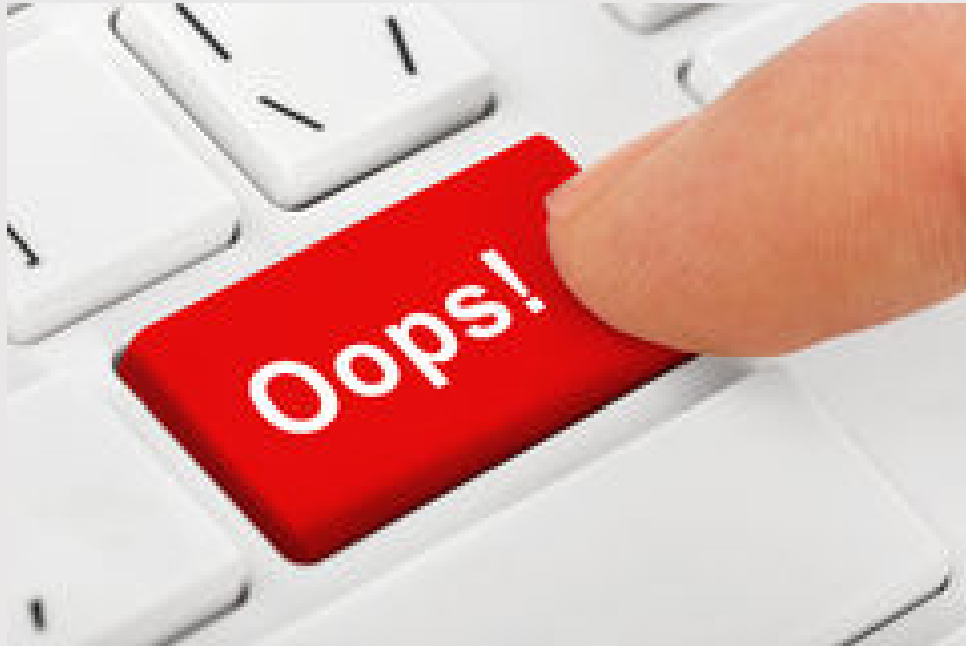




# Breach notification

- GDPR introduces a duty to report certain breaches
- Definition of breach is wider than 'data loss' (unauthorised disclosure / access / alteration)
- Must notify where '..a risk to rights and freedoms of individuals'
- Assess on case by case basis
- Must notify within 72 hours
- If 'high risk' must also notify data subjects 'without undue delay'





A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This means that a breach is more than just losing personal data.



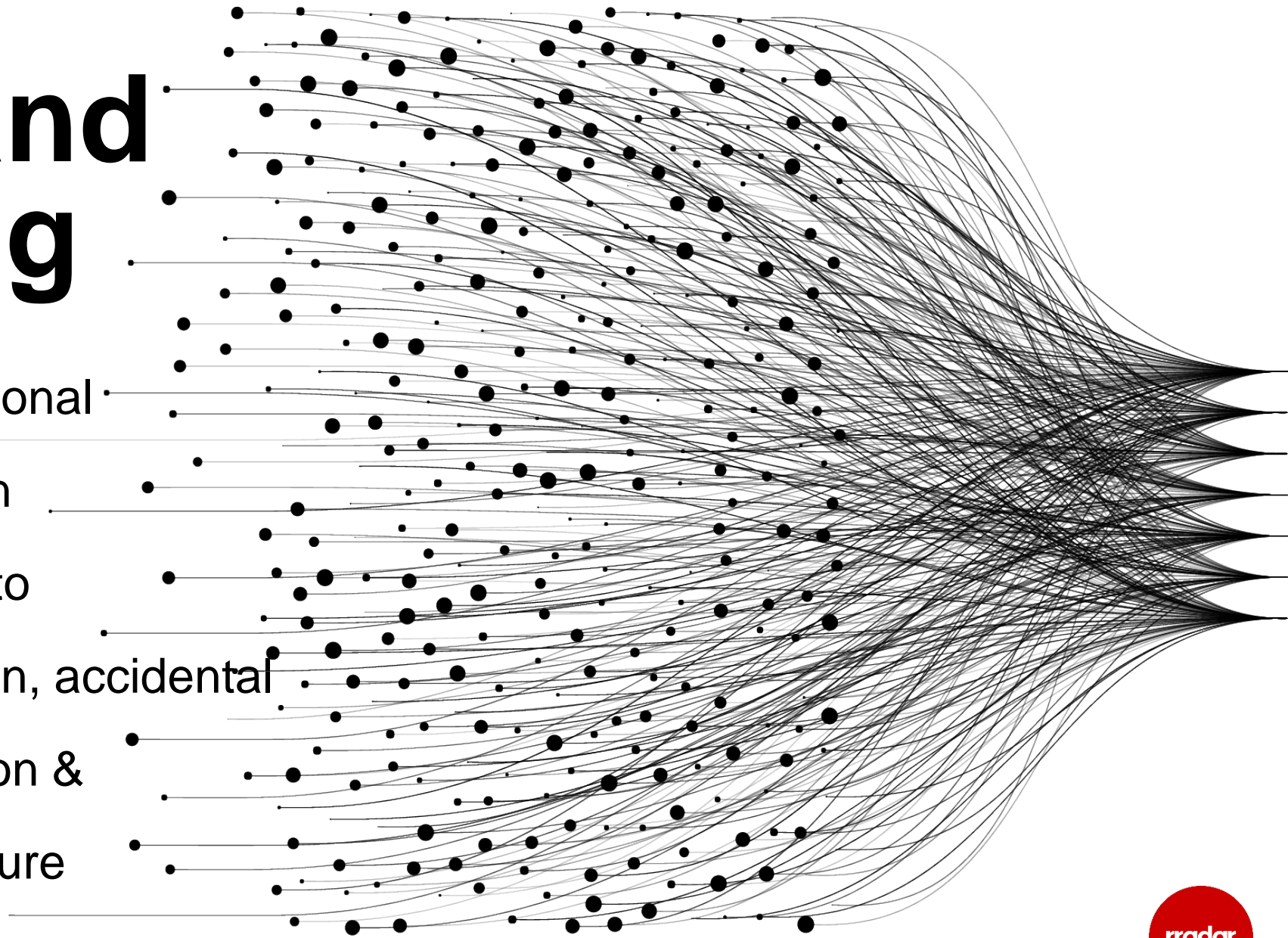
# What information must a breach notification contain?





# Security and Processing

- Technical and organisational measures must be taken
- Pay particular attention to
  - Risk of loss, alteration, accidental or unlawful destruction & unauthorised disclosure



# Regulatory Penalties

- Lots of scare stories



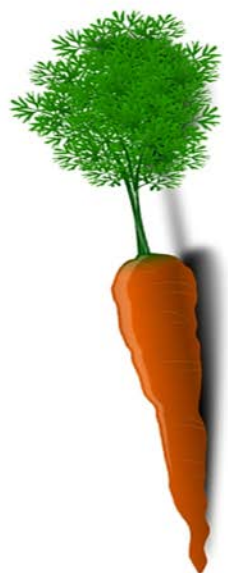
Information Commissioner's Office





- €10m or 2% turnover
- €20m or 4% turnover





**VS.**



# **Impact on the insurance profession**



# DATA MANAGEMENT



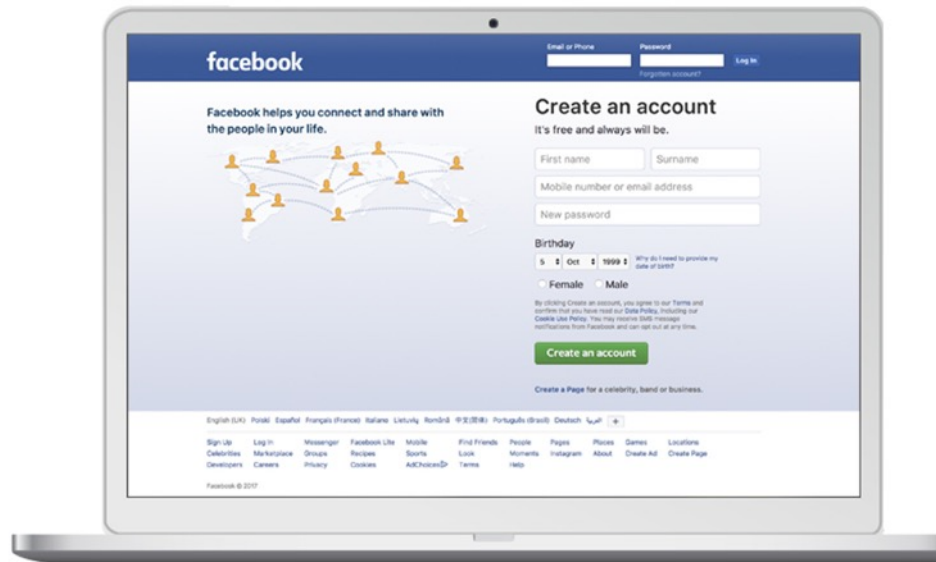


# THE RECRUITMENT PROCESS

- Screening
- Friending
- Job Description

# MONITORING SOCIAL MEDIA USE

There will be instances where an employer can be fully justified in accessing social media.




- Company Policy
- Reputation Management
- Defamation
- Copyright



# DATA BREACHES



- 
- Aggravating and Mitigating Features
  - Employment Management
  - Indiscriminate Monitoring



# VEHICLE USE

- Tracking •
- Notification •
- Personal Driving •







# THE DISCIPLINARY PROCESS

- Data as Evidence
- Access Requests
- GDPR 2018 Changes

# Practical Steps

**Act now - Be proactive - Develop a plan**



Policy review / IT enhancements / Policy updates / Privacy statements / Staff training / Data sharing agreements



Refer to ICO guidance – updated regularly (‘li

# 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

### Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7

### Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8

### Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any 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 ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11

### Data Protection Officers

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

12

### International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

# Any questions ?

**Alan Hornby**  
Chartered Insurance Practitioner

alan.hornby@rradar.com

07701 007 479



**@rradarAlan**