Privacy and Progress:

Better Futures & data privacy law compliance

presented by Heather Jack, HJBS Ltd

Supporting Better Futures for All

The Lighthouse, Glasgow

Thursday 22nd November 2018

Session outline

- Introduction to key themes – 15 minutes
  - Accountability – say it, do it, prove it
  - Risk-based approach
  - Explicit processing purposes & lawful bases
  - Right to be informed & privacy notices
  - Data controller–processor relationship
- Break-out sessions – 25 minutes
- Groups feedback and discussion – 20 minutes

Key areas of GDPR change

New **"accountability"** principle – say what you're doing, do it, prove it!

Direct data processor obligations – regardless of global location

Enhanced data subject rights – including right to be informed

Big fines & easier to get compensation

72 hours to notify serious breaches

Privacy by design & data protection impact assessments

Data Protection Officer

Explicit lawful basis for processing

Explicit emphasis on risk-based approach

Data Protection Act 2018

- Supplements GDPR for activities in scope
  - E.g. definition of a public authority
  - Bases and conditions for processing special category data
- Extends GDPR to out of scope processing
  - E.g. national defence/security
  - Additional conditions for processing criminal conviction data
- Implements EU Law Enforcement Directive
- Details ICO powers including fees regime
- Also came into force 25th May 2018

1a. Lawfulness, fairness & transparency

1b. Purpose limitation

1c. Data minimisation

1d. Accuracy

1e. Storage limitation

1f. Integrity & confidentiality

Accountability

2. The controller shall be responsible for, and be **able to demonstrate** compliance

Accountability

- Key fundamental change under GDPR
- Say it, do it - consistently, prove it
- Justify and document decision making
  - Legitimate interest assessments
  - Decision not to
    - release personal data under data subject access request
    - rectify/delete personal data under rectification/erasure request
    - Stop processing personal data

What evidence do we need?

Records of processing activities	Policies and procedures	Training records	Data protection impact assessments
Data sharing and processing agreements	Privacy notices	Proof of lawful consent	Breach log, assessment and notification
Personal data maps	Risk assessments	Adequate security measures & controls	Retention schedules & proof of compliance

Risk-based approach

Main risk areas (inter-related)

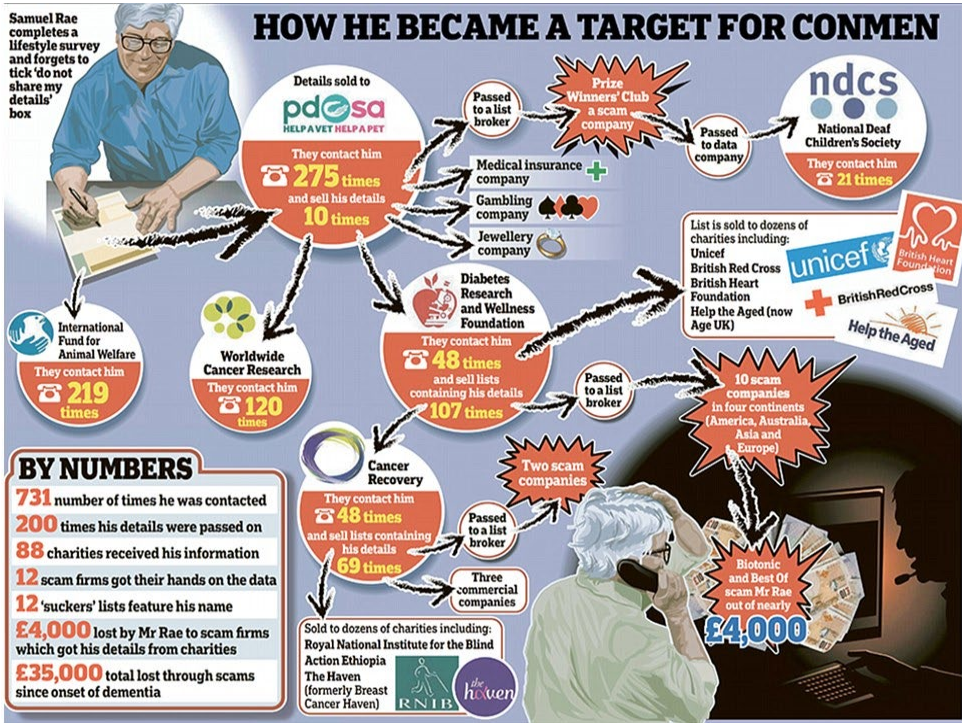
- Security – confidentiality, integrity, availability
- Records management – key to accountability
- Data sharing & disclosure

Generally related to

- Inadequate processes
- Poor governance
- People issues

Impact of risks

- Individual
  - Physical/mental harm & financial loss
- Legal
  - Litigation
- Reputational
  - Loss of trust
  - Negative media coverage
- Operational
  - inefficiency
- Financial
  - Compensation claims
  - Fines



Personal data processing risks

- Over-retention of data and records due to absence or non-compliance with retention policy
- Transmission of sensitive data to incorrect recipients
- Malware attacks on networks leading to loss or corruption of personal data
- Loss of mobile devices or removable media containing personal data
- Inadequacy of privacy notices on website and points of data capture
- Lack of controls for mobile and homeworking
- Non-reporting of information security breaches
- Failure to take account of privacy risks & requirements in organisational change projects

How do you or could you reduce the risks of these things occurring?

Processing purposes & lawful bases

Why are you processing personal data in Better Futures

Purposes & lawful bases

"For Better Futures, the reason for collecting and using personal data is to enable the provision of support for the individual and for informing future service improvement."

Generic statement from Better Future Data Protection and Privacy Policy, section 6.3

The Better Futures framework & system are tools to support your processing purposes ie delivering and improving housing support services

Lawful bases for processing

Article 6: - all personal data

a) *the data subject has given **consent…***

b) *necessary for the performance of a **contract** to which the data subject is party…*

c) *necessary for **compliance with a legal obligation…***

d) *necessary in order to protect the **vital interests** of the data subject or of another natural person;*

e) *necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority;*

f) *processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.*

- ***Point (f) shall not apply to processing carried out by public authorities in the performance of their official tasks.***

Special categories – Conditions for processing

Explicit consent	Employment law	Vital interests no consent	Special category group use
Made public by subject	Public interest underpinned by law	Establish / defend legal claims	Health / social care
	Public health	Archiving / research with safeguards	

Must specify condition under UK DP Act 2018

- Business function – housing support
- Processing purpose - explicit
- Types of personal/special category data processed
- Lawful basis for processing
- Data subject(s) & how are they are informed
- Location(s) – Better Futures system (& where else?)
- Access & ownership -
- Data flows – in, through and out of the organisation
- The source of the data – data subject, 3rd party, already held
- Third party sharing – who, why and how
  - Processors – HSEU, Regulators – Care Inspectorate, Partner agencies - ….
- How long is it kept for – life-cycle retention
- How is it protected

Privacy Notices

New data subject “right to be informed”

- When collecting data provide the following information
  - Identity/contact of data controller (and DPO where appropriate)
  - Purposes and legal basis of processing
  - Data sharing recipients and sources
  - Overseas transfer & protections
  - How long data will be stored
  - Data subject rights (including withdrawal of consent if relevant)
  - Right to complain to ICO
  - Whether providing data is a requirement & consequences of failure to provide
  - Automated decision making/ profiling

Privacy notices

- Easily accessible, plain English
  - Challenging given information that needs to be provided
- Take a layered approach to informing data subjects
  - Over-arching “full” privacy notice
    - Summary with links to more detail where required
    - Publish on website, intranet, downloadable/hard copy
    - Use videos, infographics, posters in public areas
  - Individual notices for explicit purposes at point of capture
    - Online & paper forms – link to full privacy notice
- Keep a privacy notice register for compliance evidence

Data Controllers & Processors

- Documented instructions from controller
- Confidentiality obligations
- Data security
- Sub-contracting
- Assists controller with rights and security
  - Subject access requests
  - Data protection impact assessments
  - Data breach management
- Deletes or returns data
- Records to demonstrate compliance

Final message 1

This is an opportunity for improvement

improvement

Customer service & professional ethics

- Respecting the privacy of individuals
- Earns trust of the people you support. employees & other stakeholders

Corporate governance

- Integrates privacy into “business as usual”
- Supports openness, accountability & risk
- Business improvement
- Streamline processes
- Increase efficiency

Information governance

- Security
- Retention & disposal
- Data quality
- Record keeping
- Search & retrieval
- Model for managing your information

Final message 2

25 May was the real start of the compliance journey and there ain't no perfect destination

- we are still awaiting more formal guidance from the UK and EU regulatory bodies
- we still have **no** legal precedents
- existing examples are guess work
- aim for continuous proportionate practical improvement …….. not perfection

DON'T PANIC!

KEEP CALM AND CARRY ON

Break-out session

- Each table has 20/25 minutes to discuss two data protection topics
- Select from the list or decide on alternative topic(s)
- Please take notes of discussion
  - These will be collated and a summary document produced for distribution
- Break-outs will be followed by topic feedback and further discussion