Beacon Authority
2008 - 2009
Reducing Re-offending
2003 - 2008
Winner of 6 previous Beacon Awards

TOWER HAMLETS

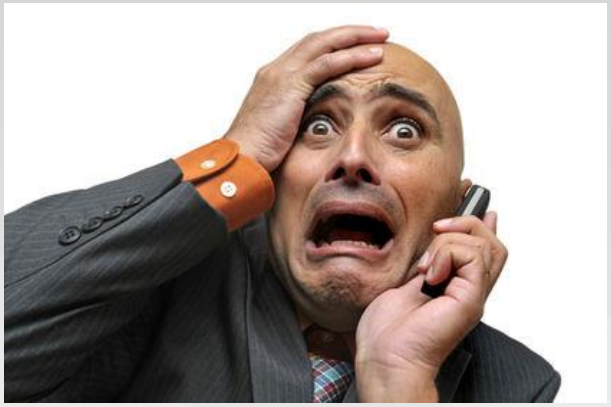
General Data Protection Regulation (GDPR) Training for Adult Social Care Providers

Redouane Serroukh
Information Governance Manager
Children's and Adults Services

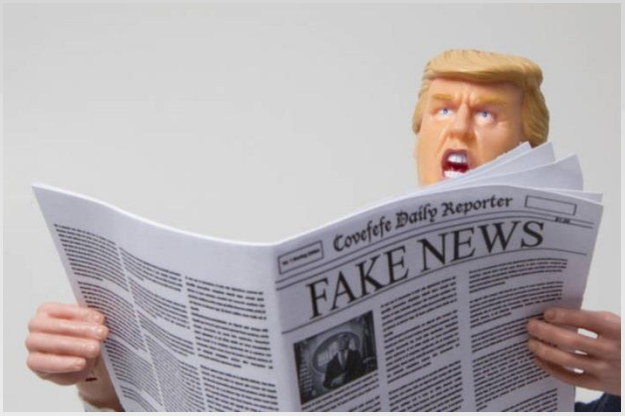
Agenda

- What is new in the GDPR?
- The (new) rights of individuals under the GDPR
- Privacy Notices
- Consent
- The Data Protection Officer role
- Contracts and procurement
- Data breaches and fines

GDPR?.....Should I Panic?

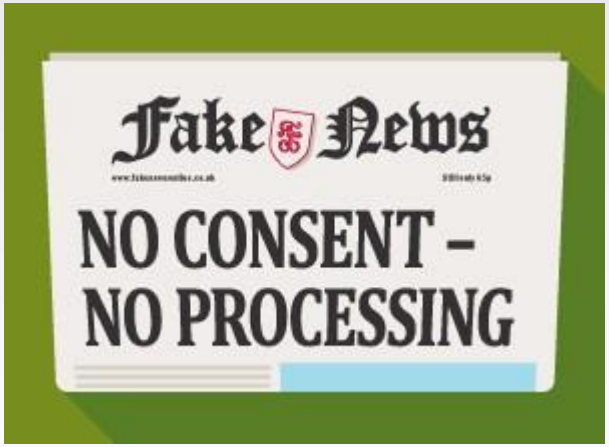


What do you know about GDPR?

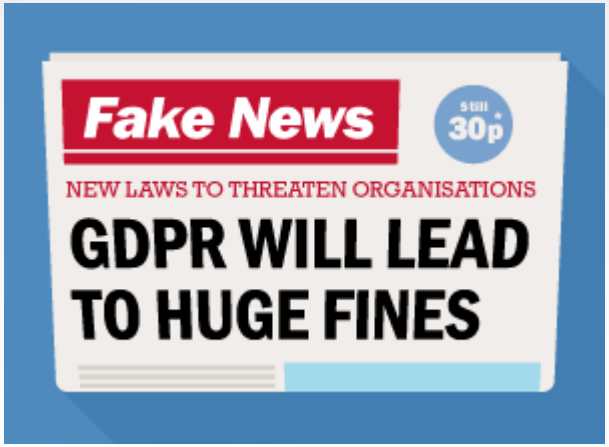


"GDPR will not matter after we leave the EU"

"We're only a small organisation; GDPR doesn't apply to us"



"Its going to be like Y2K
Lots of hype and nothing will happen"



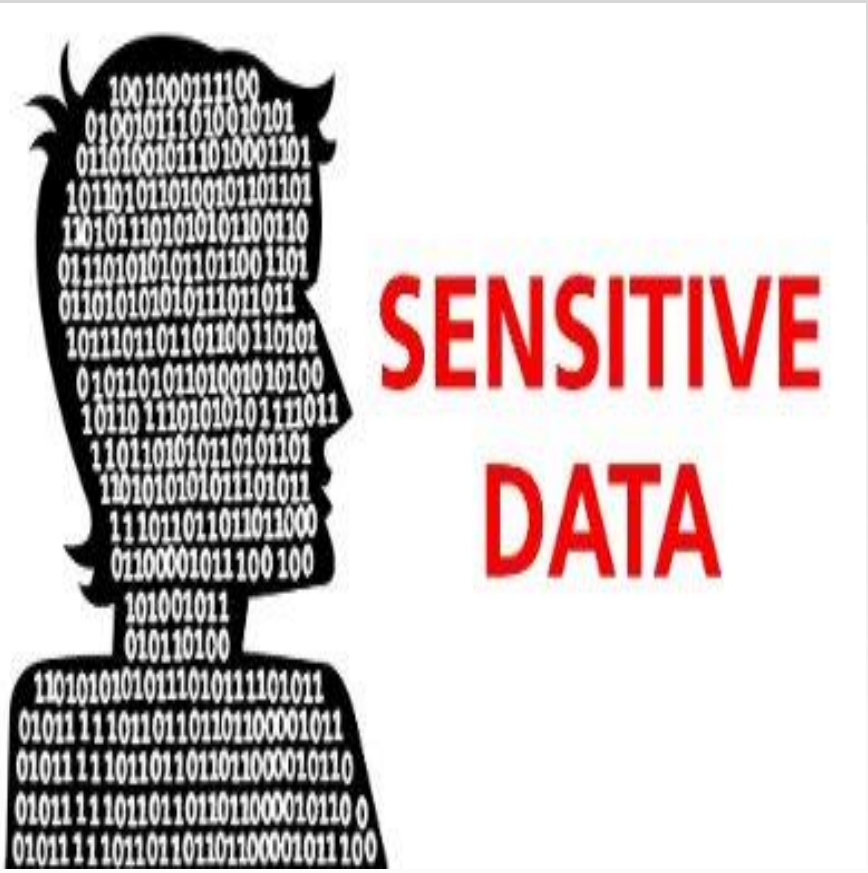
So what is GDPR?

- European General Data Protection **Regulation** - not Directive
- Comes into force on 25th May 2018
- Brexit!?
- Replaces the Data Protection Act 1998
- Covers all European citizens
- The Data Protection Bill – filling in the blanks
- Information Commissioner's Office
- The value of personal data

What's new in GDPR?

- Europe wide – consistency
- Clearer Consent
- Enhanced rights for individuals
- Data Protection by Design / Privacy Impact Assessments
- Stronger Penalties (Eye watering!)
- Mandatory breach reporting
- Mandatory Data Protection Officers
- ACCOUNTABILITY

Personal or Sensitive (Special Categories)



What is Personal Information?

What kind of Information do you hold?

- Personal and sensitive information
- Information on the extended
- Staff details (including log in details)
- Third party agencies' information and contracts
- Financial information
- Biometric
- Pictures

What format do we hold it in?

How do we hold this information?

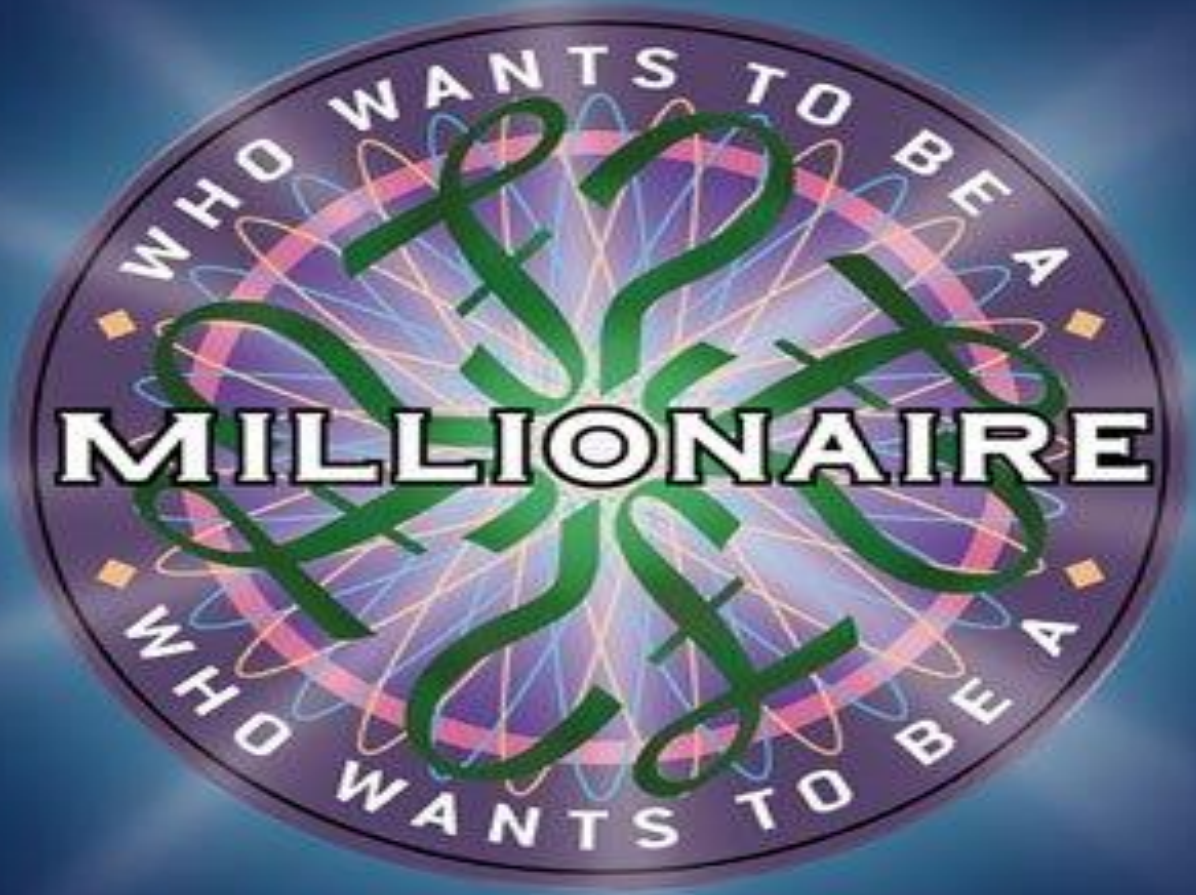
- Paper
- Electronic files
- Databases
- Email
- CCTV / Audio files
- Post it notes!

The 6 GDPR Principles

Require that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and not excessive.
- Accurate and kept up to date.
- Held for no longer than necessary.
- Processed in a manner that ensures appropriate security of the personal data.

Who wants to make the **ICO** a Millionaire



You are required to send personal data to a client or the Council, do you…


A. Send it via Hotmail as secure email is too expensive

B. Order a chest, metal chains and padlocks and courier to client

C. Leave the file at a tube station ‘lost and found’ for client to collect

D. Send via Encrypted email (Egress)

Conditions for processing personal data

- Consent
- Necessary for contract
- Necessary for a legal obligation
- Vital interests (in absence of other conditions)
- Necessary for official authority/ task carried out in the public interest
- Necessary for legitimate interest

Conditions for processing 'special categories' data

- Explicit consent
- Necessary for field of employment and social security.
- Vital interests where person physically or legally incapable of giving consent.
- Manifestly made public by data subject
- Necessary for the establishment

Data Subject Rights

- A Data Subject is the legal term for an individual
- All requests must be processed within 1 month.
- Clock starts after the requestor has made a valid request, which includes being ‘verified’

- Subject Access Requests
- Right to rectification
- Right object

- Right to be forgotten (erasure)
- Right to Restriction
- Right to data portability

Privacy Notice

- A Privacy Notice is the statement or disclaimer that is added at the end of application forms or given as a leaflet
- Also known as Data Protection Statement or Fair Processing Notice
- Includes information about why information is being collected and who may be shared with and used for

Privacy Notices

Must now include:

- ID of Data Controller
- Contact details of DPO
- Purpose and legitimate basis for processing
- Who data is shared with
- Retention period
- Data Subject rights to be made clear, including rectification /portability objection
- Right to withdraw consent if relied upon

A Police Officer shows their badge and asks for Information about a family in a non urgent case , do you…


A. Quickly provide them with everything you have….it's the Police!

B. Ask the Officer for a written request

C. Thoroughly inspect the badge and uniform and ask the officer to confirm it was not from ebay

D. Provide the information on condition they don't say it was from you

Consent

- Must be evidenced and can demonstrate compliance with the conditions of consent.
- Must be able to withdraw consent at any time
- Don’t ask for consent if your going to do that thing anyway!
- What are they signing or agreeing to?

Contracts and Procurement

- As part of our compliance we will need to ensure you are compliant
- Need to have assurance that the organisation is compliant with GDPR before entering into a contract
- You could be liable for lack of good procedures and checks if contractor breaches privacy or losses data
- We may need to review your current contracts

The Data Protection Officer (DPO)

- Required by Public authorities and public bodies.
- ….and any Org that is involved in large scale monitoring or processing of special categories data.
- Organisations with a group structure can have a single DPO
- A joint DPO can be appointed for public authorities
- External DPO can be contracted
- Must have “expert knowledge of data protection law and practices”

The DPO's Tasks

- Advise the organisation and staff on obligations under GDPR
- Monitor compliance with GDPR, Data Protection Laws and Organisation's own policies
- Provide advice on Impact Assessments and monitor performance
- Cooperate with ICO on GDPR issues and act as contact point with them

You have printed out an extra copy of a client's file that is no longer needed, do you…


A. Leave it for the cleaner to throw away

B. Save the trees and reuse the paper for scrap notes or paper airplanes

C. Securely shred or dispose of the file

D. Throw it in the bin or skip on the way home as the office bin is full

Information Security Breach

- You need to have ‘appropriate’ security measures to protect data from:
- Accidental or unlawful destruction
- Loss
- Unauthorised disclosure
- Unauthorised Access

Breach Notification to the ICO

- If the breach is likely to cause high risk to rights and freedoms of subjects:
- Breach must be reported to ICO within 72 hours.
- Should include name / contact details of DPO, likely consequences of breach and measure taken to mitigate risk

ICO Fines

- Previously under Data Protection Act max fine of £500,000
- Under GDPR max fine is €20,000,000 or 4% of global turnover, which ever is higher.
- Lower fine of €10,000,000 or 2% for breach of the Regulation (procedures).

End of Session
Thank you for attending