

# General Data Protection Regulations & Info Sharing



# Objectives

- ◆ GDPR compliance
- ◆ Information Sharing

# Cambridgeshire and Peterborough Information Sharing Framework

## Members

## Cambridgeshire and Peterborough

- **Local authorities**
- **Health**
- **Police**
- **Fire**



Cambridgeshire  
Information  
**Sharing**  
Framework

# Cambridgeshire and Peterborough Information Sharing Framework

- ◆ Framework
- ◆ Sharing charter
- ◆ Information sharing templated agreement
- ◆ IG Professionals



# GDPR Background

- ◆ New EU Regulation – to be adopted in full by all EU member States so as to harmonise Data Protection across Europe.
- ◆ Does Brexit change it - No
- ◆ The Data Protection Bill going through parliament.



## Regulations need to become UK law



Areas still need to be decided upon, eg:

- Data Subject rights exemptions
- Freedom of expression and freedom of information;
  - Public access to official documents;
- Age when children can access online service without parental consent
- Processing of health & social care data

# Moving from DP to GDPR

- ◆ Building on what is currently good practice under the **Data Protection Act**.
- ◆ Makes some of this good practice **mandatory** and significantly increases the **penalties for non-compliance**.
- ◆ **Increased collection and use of data** means that legal framework is more important than ever before

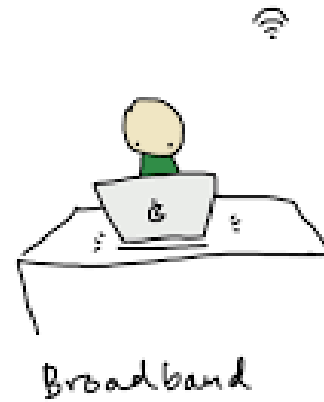


# Main changes include

- ◆ **Accountability**
- ◆ **Data Protection Officer**
- ◆ **Enhanced rights for individuals**



# Replacing Data Protection Act 1998



# 2018



## Personal Data

“Data which relates to a living, identifiable individual, that is biographical in nature and has them as its focus”



Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

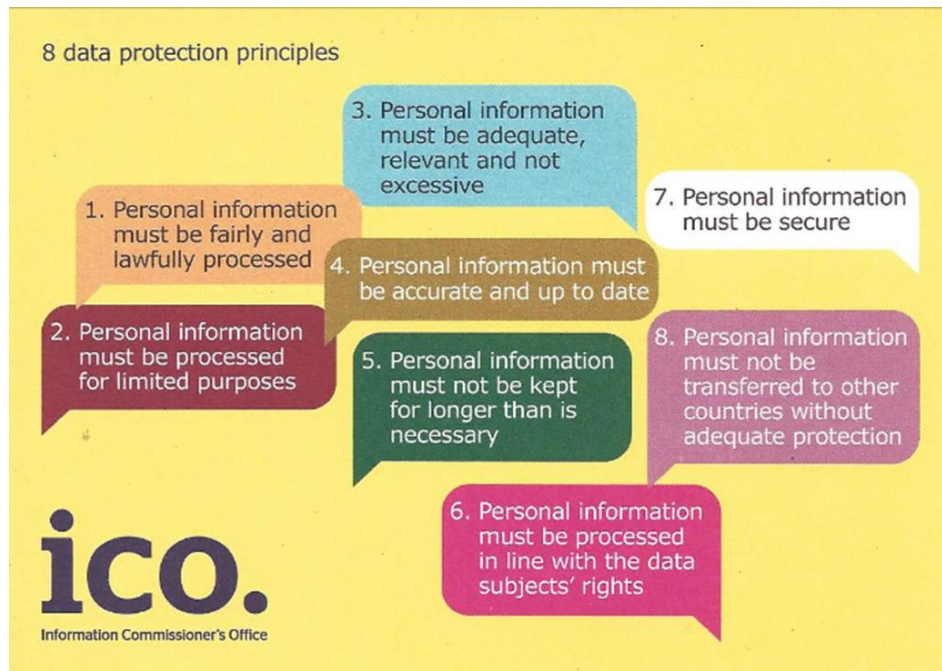
Data Processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

# Special personal data

- ◆ race
- ◆ ethnic origin
- ◆ politics
- ◆ religion
- ◆ trade union membership
- ◆ genetics
- ◆ biometrics (where used for ID purposes)
- ◆ health
- ◆ sex life or
- ◆ sexual orientation.

# Revised Principles

## DPA – 8 principles



## GDPR – 6 principles

- ◆ Fair & lawful
- ◆ For specific, explicit and legitimate purpose
- ◆ Adequate, relevant & limited
- ◆ Accurate & up to date
- ◆ Not kept longer than necessary
- ◆ Ensure appropriate security
  
- ◆ PLUS whole new section on individual rights

# GDPR – Enhanced Rights for Data Subjects

## Right to be informed

- Explain to people what we are doing with their data in a clear and concise way.

## Right to access

- Provide a person's own data for free and ask them to specify what they want

## Right to rectification

- A person can ask us to amend data if it is inaccurate or incomplete

## Right to Erasure

- A person can ask for information to be deleted in certain cases, for example consent withdrawn or no longer needed

## Right to Restrict

- We can be asked to block processing, in certain situations, for example the accuracy is contested or no longer needed

## Right to Data Portability

- We should be able to provide data back to people in a way in which they can re-use it but only in certain cases

## Right to Object

- A person can object to processing activities for example those based on public interest or official authority

## Right on Automated Decision Making

- We can be asked to make a “human decision” rather than by an automated process. This also applies to profiling.

## Key areas that will have an impact

1. Recording what personal data we've got
2. What we tell people about how we use their information
3. Consent
4. Data Protection incidents/breaches
5. Privacy by Design
6. Contracts, third parties and IT systems

# 1. Recording what personal data we've got

- ◆ Review and update your **Information Asset Register**
  - ◆ list all of our key assets
  - ◆ to show you know what information we have, and have good control over it
- ◆ Need support from asset owners in services
  - ◆ to ensure everything is captured
  - ◆ need to keep this under review.



## 2. What we tell people about how we use their information

A **Privacy Notice** should explain why we collate the info and how we will use it. We already do this, but GDPR increases the requirements. We need to tell people

- ◆ Our lawful basis for processing the data,
- ◆ Data retention periods
- ◆ Data sharing
- ◆ Data subjects have a right to complain to the ICO
- ◆ DP Officer Contact Details
- ◆ ...and more!

Must use clear and plain language when explaining consent.

# Data Protection Officer



All public Bodies must appoint a DPO

This is a statutory position

Must be experienced and qualified to take on the role

Can be outsourced

# Other GDPR conditions

- ◆ Data Breaches
- ◆ Privacy by Design
- ◆ Contracts and procurement
- ◆ IT systems

## 3. GDPR Consent – new standards

If we rely on Consent to process information we need to meet new standards :

Consent must be:

- ◆ Freely Given
- ◆ Informed
- ◆ Unambiguous
- ◆ Explicit
- ◆ Affirmative
- ◆ Recorded - Must show an audit trail
  
- ◆ And it can be withdrawn!



## 3. Consent – what is it?

GDPR changes rules around consent. But, need to understand what we mean by consent in this context.

This is not about consent to work with us, or consent to receive a service.

FOR GDPR Consent - **legal basis** for processing information

**As a public authority, generally we have a specific legal basis for processing; therefore we don't need consent and should not mislead by asking for it.**

### 3. Consent – Just one of Conditions for Processing

There are revised conditions for processing data and for processing non-special personal data under GDPR these are:

- ◆ Contract
- ◆ Legal obligation
- ◆ Vital interest of data subject
- ◆ Public interest/task
- ◆ Legitimate interest
- ◆ (Consent)



# Conditions for processing..

Conditions for processing **special** category data under GDPR:

- ◆ Explicit consent
- ◆ Employment, social security or social protection law
- ◆ Vital interest of data subject or another
- ◆ Not-for-profit bodies
- ◆ Made public by data subject
- ◆ Legal claims
- ◆ Substantial public interest
- ◆ Medicine, health or social care
- ◆ Public health
- ◆ Research and statistics
- ◆ + national derogations

# Power to process personal data

- ◆ Article 9 2 (g)
- ◆ processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to **safeguard** the fundamental rights and the interests of the data subject;

# Power to process personal data

- ◆ Article 9 2 (h)
- ◆ processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, **the provision of health or social care** or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

# Legal basis

The legal responsibilities of Boards and statutory duty for agencies

- ◆ Care Act 2014 (Sections 43 to 45) for adult safeguarding and
- ◆ Children and Social Work Act 2017 (Sections 16E to H) for children and young people.

# Information Sharing Barriers

- ◆ Excessive caution – consequences of data misuse
- ◆ Lack of assurance
- ◆ Technology
- ◆ Knowledge
- ◆ Different cultures and legal interpretations
- ◆ Personnel

# Information Sharing Barriers

- ◆ Resources
- ◆ Fundamentals
- ◆ Bureaucracy & Inflexibility
- ◆ Stakeholders
- ◆ Time
- ◆ Legislation

# Share or not

Myth – Data Protection says you can't share data.

**WRONG!**

# Power to share



# What to do

- ◆ Engage with your Data Protection Officer/  
IG team
- ◆ Engage with partners
- ◆ Revised Information sharing agreements
- ◆ Revisit procedures
- ◆ Train staff

# Get in contact

## Information and Records

[Data.protection@Cambridgeshire.gov.uk](mailto:Data.protection@Cambridgeshire.gov.uk)

01223 699137

# GDPR - What you need to do next

Consider whether you and your organisation have to do:

1. Information Assets
2. Privacy notices
3. Consent
4. Data Breaches
5. Training
6. Privacy by design
7. Contracts and third parties
8. IT systems