



GENERAL DATA PROTECTION REGULATIONS - LOVE IT OR LOATHE IT

Ron Ruston

Partner

9 March 2018

Kennedys



# Overview

Background to the GDPR	3 - 10
GDPR - Overview	11 - 13
Accountability, Fines and DPO	14 - 23
Consent	24 - 32
Other lawful bases for processing data	33 - 44
Summary	45 - 59



# BACKGROUND TO THE GENERAL DATA PROTECTION REGULATION

# Background to the GDPR



- ❑ General Data Protection Regulation (GDPR) comes into force on 25 May 2018
- ❑ Will build on the current Data Protection Act 1998



## Why the need for Change?







# Background to the GDPR

## Data records in 1988

### Data Protection Act 1998

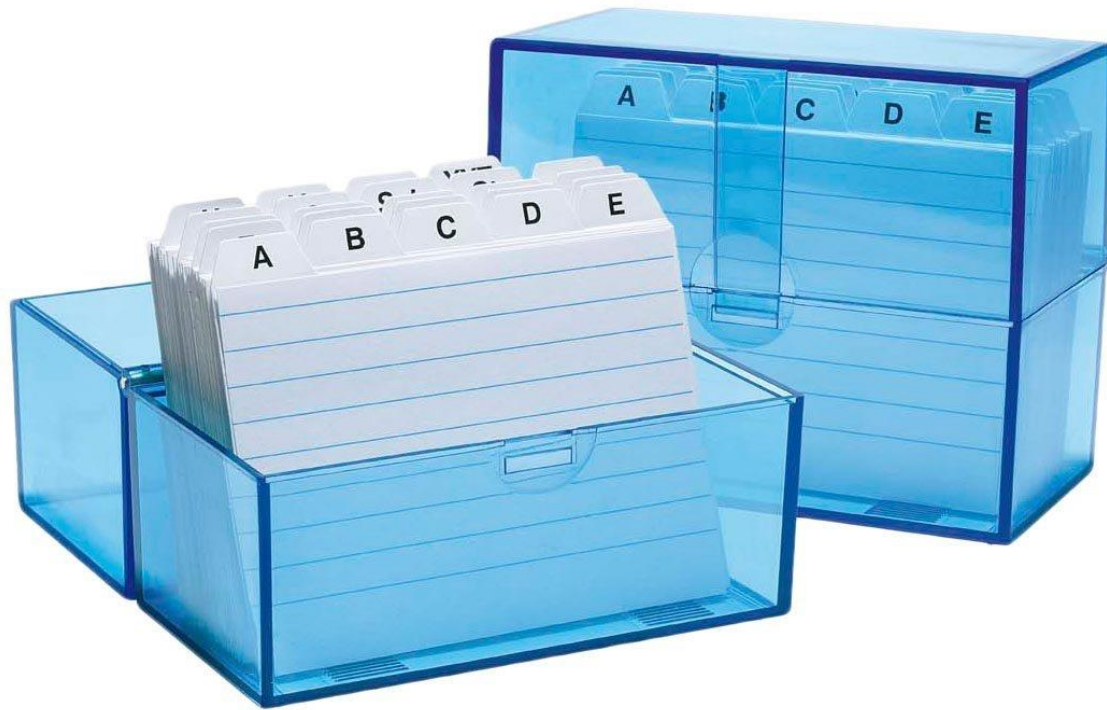
The Data Protection Act was brought in to protect personal data stored on **computers or in an organised paper filing system.**

- Filled in forms
- Records were kept in paper files
- Processed and then destroyed after 6 years

# Background to the GDPR

## Data storage in the late 80's and 90's

Personal data on a paper database





# Background to the GDPR

Storage of personal contacts



Now we do not dispose of data.







# GENERAL DATA PROTECTION ACT OVERVIEW

# GDPR

## Overview

### What is the new GDPR?

GDPR is the new data protection regulation that comes into effect in May 2018

### What does it mean?

It means you have to manage and protect personal data that you hold.

### Why do we need to comply?



1. To avoid potentially heavy fines from the Data Commissioner
2. To reduce risk of legal action from individuals in the event of unauthorised use.





# GDPR

## The GDPR...

- Applies equally in all member states
- Makes organisations accountable
- Is catching up with technology
- More than just a tick boxing exercise  
- Means bigger fines for organisations that get it wrong
- Failure to comply can lead to both financial and reputational costs





# ACCOUNTABILITY, FINES AND DPO



# GDPR

## Accountability

### Biggest change - Accountability

- How we store data
- How we share data
- Audit trail
- Inaccurate information



# GDPR

## Privacy Information

- Keeping personal data safe
- Privacy notice/ Privacy impact statement
- Lawful process for processing data



# GDPR

## Failures in keeping Personal Data Safe

### ❑ Samira Bouzkraoui - Prosecution

- Bouzkraoui took a screenshot of a Council spreadsheet concerning children and their eligibility for free school meals and sent it to a parent via snapchat.
- Images included names, addresses, and DOBs of 37 pupils and their parents.
- Fined £850.00 plus £713.00 costs



# GDPR

## Failures in keeping Personal Data Safe

### ❑ Woodgate & Clark fined

- Data related to a claim on an insurance policy in relation to a business premises.
- Private investigators unlawfully obtained confidential financial information, including details of bank transactions and disclosed it to Woodgate & Clark, who then disclosed it to their insurance client.
- Woodgate & Clark convicted of 2 counts of unlawfully disclosing personal information.
- Fined £50,000.00 plus £20,000.00 in costs.

# GDPR

## Increase in fines

- ❑ Increase from £500,000.00 cap to...
- ❑ Up to 20 million Euro in potential fines or
- ❑ 4% turnover (whichever is higher)





# GDPR

## Data Breaches

- Under current UK Data Protection most personal data breach reporting is best practice, not compulsory
- Requirement for organisations to report a personal data breach that affects peoples rights and freedoms not later than 72 hours after having become aware of it.
- Report to include potential scope and the cause of the breach



# GDPR

## Avoiding Breaches

### ❑ Best practice for avoiding breaches:

- Robust systems
- Hacktavists
- Password protection
- Staff training

# GDPR

## Data Protection Officers

When must you designate a Data Protection Officer?

- Are a public authority; or
- Carrying out a large scale systematic monitoring of individuals; or
- Carrying out large scale processing of special categories of data or data relating to criminal convictions and offences.

AND....

- Any organisation is able to appoint a DPO as companies must ensure sufficient staff to discharge responsibilities under GDPR.





# GDPR

## Data Protection Officers

### What are the tasks of a DPO?

- Inform and advise organisation and employees about GDPR obligations;
- Monitor compliance with the GDPR and other data protection laws;
- Advise on data protection activities, advise on data protection impact assessments and conduct internal audits;
- Be the first point of contact for supervisory authorities and for individuals whose data is processed.





**CONSENT**

# GDPR

## Lawful Processing - Consent

### DEFINITION OF CONSENT:

Consent means:

- ❑ freely given;
- ❑ Specific;
- ❑ Informed;
- ❑ Unambiguous; and
- ❑ Explicit

# GDPR

## Lawful Processing - Consent

### (A) Freely given

GDPR confirms it will not be freely given if:

- The data subject has no genuine and free choice;
- Is unable to withdraw or refuse consent without detriment, and/or:
- There is a clear imbalance between the parties. Examples of where it will not be deemed to be freely given:
  - Sought by the individual's employer;
  - Sought by a local authority;
  - If the performance of a contract is conditional on the data subject's consent to processing.



# GDPR

## Lawful Processing - Consent

### (B) Unambiguous

GDPR requires an express clarification by either statement or clear affirmative action in order to be valid.

Should include:

- Ticking a box in an online context;
- Any statement or conduct which clearly indicates the data subject's acceptance of the proposed data processing activities.

# GDPR

## Lawful Processing - Consent

### (C) Specific

- Must relate to specific processing operations.
- A general broad consent to unspecified processing operations will be invalid.

# GDPR

## Lawful Processing - Consent

### (D) Informed

- Data subjects should understand the extent to which they are consenting and;
- Be aware, at least, of the identity of the controller and;
- The purposes of the relevant processing.

### (E) Right to Withdraw

- Data subjects must be able to withdraw their consent at any time and be informed of their withdrawal;
- Withdrawing consent must be as easy as giving it.

# GDPR

## Lawful Processing - Consent

### (F) Formal Requirements

Consent may be:

- in writing, including in electronic form, or oral form.
- CAUTION should be exercised when relying on oral consents as the onus for demonstrating that consent has been obtained clearly is on the controller.



# GDPR

## Overview - Consent

- GDPR sets a high standard for consent;
- Means offering individuals genuine choice and control;
- Has to be freely given;
- Requires a positive opt-in. Does not include pre-ticked boxes/ opt outs/ children's consents;
- Requires explicit consent - must be a clear and specific statement of consent;

# GDPR

## Lawful Processing - Consent

### Action for businesses intending to rely on consent....

- Identify all their processing activities which are legitimatised through data subject consents;
- Consider whether it makes sense to rely on consents in all those scenarios, or whether other potentially safer conditions/justifications can be relied on;
- Ensure processes are in place to promptly honour any withdrawals of consent;
- Put in place systems of creating reliable records of consents which will enable organisations to demonstrate compliance.

# OTHER LAWFUL BASIS FOR PROCESSING DATA

# GPDR

## Alternative Lawful basis

- ❑ Review existing data and ensure processing is fair
- ❑ Need to document and identify the lawful basis for processing data
- ❑ Legitimate basis for processing data set out in Article 6 (1):
  - (a) Consent (dealt with above)
  - (b) Contract
  - (c) Compliance with a legal obligation
  - (d) Protect vital interests
  - (e) Public interest
  - (f) Other legitimate interests



# GDPR

## Alternative Lawful basis

- ❑ **Article 6 (1) (b) Necessary for the performance of a contract:**
  - ❑ You have a contract with an individual and you need to process their personal data to comply with your obligations under the contract.
  - ❑ You haven't got a contract with the individual but they have asked you to do something first (i.e. provide a quote) and you need to process their personal data to do what they ask.

### Example

An individual shopping around for car insurance requests a quotation. The insurer needs to process certain data in order to prepare the quotation, such as the make and age of the car.

# GDPR

## Alternative Lawful basis

- Article 6 (1) (c) Compliance with a legal obligation**
- Processing personal data to comply with a common law or statutory obligation;
- Does not apply to contractual obligations;
- Processing must be necessary - if you can reasonably comply without processing the personal data, this basis does not apply.



### Example

An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC.

The employer can point to the HMRC website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation.

# GDPR

## Alternative Lawful basis

- ❑ Article 6 (1) (d) Processing is necessary to protect the vital interests of the subject or another natural person

### What are vital interests?

- Vital interests are intended to cover only interests that are essential for someone's life.
- Limited in scope - generally will only apply to matters of life and death.



#### **Example**

An individual is admitted to the A & E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests.

# GDPR

## Alternative Lawful basis

- ❑ **Article 6 (1) (e) Necessary for the performance of a task carried out in the public interest**

### What is a public task?

- Carrying out a specific task in the public interest which is laid down by law; or;
- Exercising official authority which is laid down by law

### When can this be relied upon?

- Necessary for the administration of justice;
- Parliamentary functions;
- Statutory functions; or
- Government functions.

# GDPR

## Alternative Lawful basis

### ☐ Article 6 (1) (f) Legitimate Interests

Three part test:

1. **Purpose test:** Are you pursuing a legitimate interest?
2. **Necessity test:** Is the processing necessary for that purpose?
3. **Balancing test:** Do the individual's interests override the legitimate interest?



# GDPR

## Alternative Lawful basis

- ❑ Substantial public interest and safeguarding
  - Vulnerable adults
  - Children

# GDPR

## Alternative Lawful basis

### Not so relevant

- Preventative medicine
- Public health
- Scientific or historical research
- Professional bodies

# GDPR

## Alternative Lawful basis

### ❑ Article 9 (2) Other basis for processing special category / personal data

- 9 (2) (a) Explicit consent - ethnic origin, religion, sexual orientation, disability.
- Other exceptions:
  - 9 (2) (b) Necessary for carrying out obligations under employment, social security or social protection law
  - 9 (2) (c) Protection of data subjects vital interests where the data subject is physically or legally incapable of giving consent
  - 9 (2) (d) Legitimate activities of a not for profit organisation

# GDPR

## Alternative Lawful basis

### ❑ Article 9 (2) Special Category Data:

- Article 9(2) (f) - Processing is necessary for the establishment, exercise or defence of legal claims or whenever Courts are acting in their judicial capacity
- Section 35 (2) Data Protection Act - Personal data are exempt from the non-disclosure provisions where the disclosure is necessary for:
  - (a)... Any legal proceedings;
  - (b)...Obtaining legal advice

# GDPR

## Alternative Lawful basis

- ❑ Organisation should choose the lawful basis that most closely reflects:
  - True nature of the relationship
  - Purpose of processing





# SUMMARY

# GDPR

## Summary - Consent

- Identify all processing activities which are legitimatised by consent.
- Where consent is relied on make sure it will be:
  - Freely given;
  - Specific;
  - Informed;
  - Unambiguous and;
  - Explicit; and
- Ensure processes are in place to promptly honour any withdrawals of consent
- Put in place systems of creating reliable records of consents which will enable organisations to demonstrate compliance with consent requirements.

# GDPR

## Summary continued

- ❑ So in reality not so different from what we do now:
  - Robust and safe systems
  - Training is key
  - Consider if Data Protection Officers should be put in place
  - Can we justify the data processing

[lco.org.uk](http://lco.org.uk)

 @KennedysLaw

 [linkedin.com/company/Kennedys](https://www.linkedin.com/company/Kennedys)

 [facebook.com/KennedysTrainees](https://www.facebook.com/KennedysTrainees)

[kennedyslaw.com](https://www.kennedyslaw.com)

Kennedys