

Data Protection Update: Preparing for General Data Protection Regulation GDPR



Naomi Matthews



Nottingham
City Council

Aims of the session



- Consider what changes the new General Data Protection Regulation will bring about
- What preparations does Nottingham City Council need to make for next May
- Look at some recent data breaches and their relevance to NCC



The General Data Protection Regulation GDPR

- Comes into force on the 25 May 2018
- Data Protection Act 1998 will be repealed
- Data Protection Bill currently in House of Lords- this supplements the GDPR.



Increased enforcement powers

- New fines will be imposed on a two tier basis
- For contraventions such as record keeping and data processor contracts, failure to notify breaches within 72 hours a fine of 2% of turnover or 10 million Euros
- For contraventions of data protection principles, data subject rights the fine will be up to 4% of annual turnover or 20 million Euros



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 Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the 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 guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officers

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

12 International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

GDPR Awareness campaign

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.

- 12 steps campaign on plasma screen
- Communications plan
- GDPR Action plan
- IMAB project plan for GDPR
- Working group- meeting on monthly basis to try and include all key stake holders



From **May 2018** the Data Protection Act 1998 will be replaced by the **General Data Protection Regulation**



Step 1: Awareness

Decision makers and key people must be aware of the changes and appreciate the impact this is likely to have



 Data Protection Team: ext. 63855

 Data.protection@nottinghamcity.gov.uk



Safe, clean, ambitious, proud



**Nottingham
City Council**

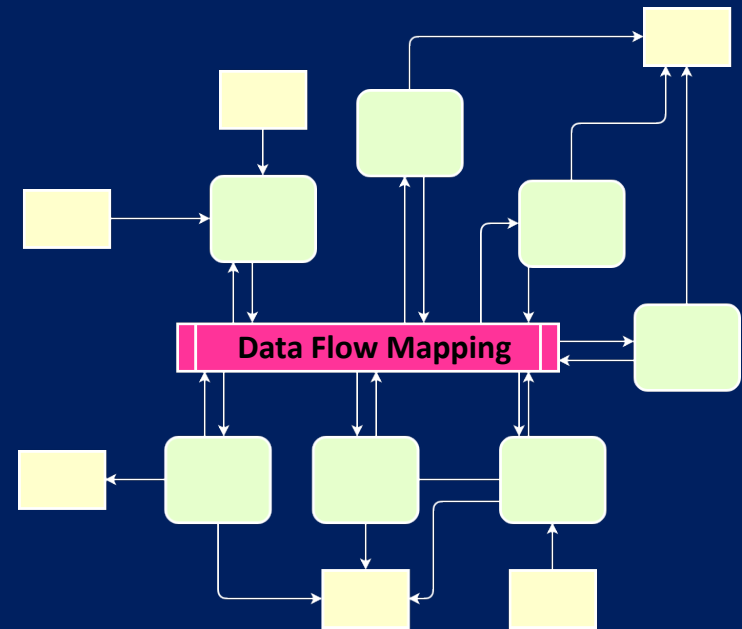
12 Steps of GDPR

Step 2: Information you hold

Every team will need to document:

- **what** personal data is held
- **where** it came from
- **who** it is shared with
- **how** it is shared (risk assessments).

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**



 **Data Protection Team: ext. 63855**
 **data.protection@nottinghamcity.gov.uk**



Safe, clean, ambitious, proud



Nottingham
City Council

12 Steps of GDPR

Step 4: Individual's Rights

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

Do your procedures cover all the rights individuals have?

- How personal data is deleted
- How it is provided
- How it is used



 Data Protection Team: ext. 63855

 Data.protection@nottinghamcity.gov.uk



Safe, clean, ambitious, proud



Nottingham
City Council



12 Steps of GDPR

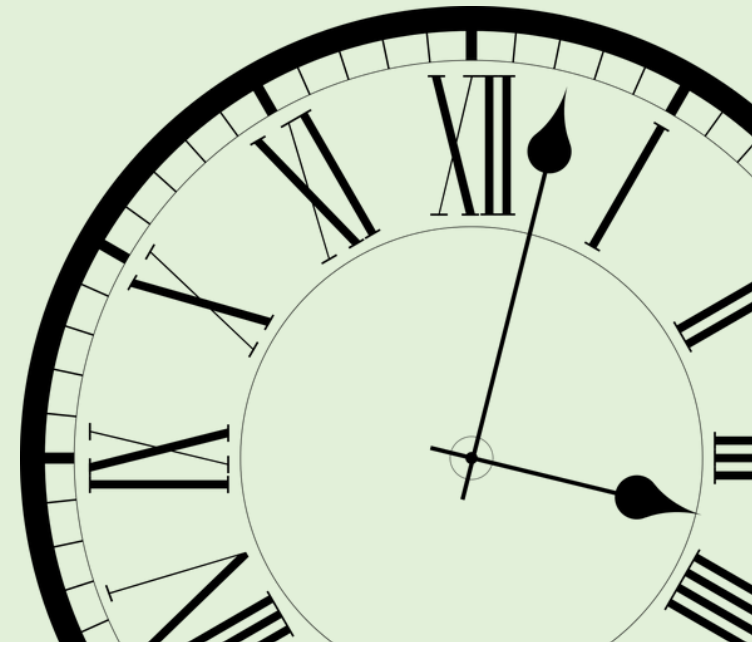
From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

Step 5: Personal information Request (PIR)

Citizens can request their personal information to be provided:

- Free of charge
- Within a month

 **Data Protection Team: ext. 63855**
 **data.protection@nottinghamcity.gov.uk**



Safe, clean, ambitious, proud



Nottingham
City Council

12 Steps of GDPR

Step 6: Lawful basis for processing personal data

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

By May 2018 you must:

- Identify the lawful basis for your processing activity
- Document it
- Update your privacy notice to explain it.



 Data Protection Team: ext. 63855

 data.protection@nottinghamcity.gov.uk



Safe, clean, ambitious, proud



Nottingham
City Council

12 Steps of GDPR

Step 7: Consent

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

You must review how you **seek, record and manage** consent. Consent must be:

- Freely given
- Specific
- Informed
- Unambiguous



 Data Protection Team: ext. 63855

 Data.protection@nottinghamcity.gov.uk



Safe, clean, ambitious, proud



Nottingham
City Council

12 Steps of GDPR

Step 8: Children

Begin to think whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any on-line website for children



 Data Protection Team: ext. 63855

 Data.protection@nottinghamcity.gov.uk

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**



Safe, clean, ambitious, proud



Nottingham
City Council

Record keeping and audit of information- Data flow mapping

- Under A 30 the organisation must maintain a record of processing operations under its responsibility
- The record should be seen as a tool to allow an overview of all the personal data processing activities an organisation is carrying out
- Prerequisite for compliance
- Effective accountability measure for the Council



GDPR – Information Audit

2

Information you hold

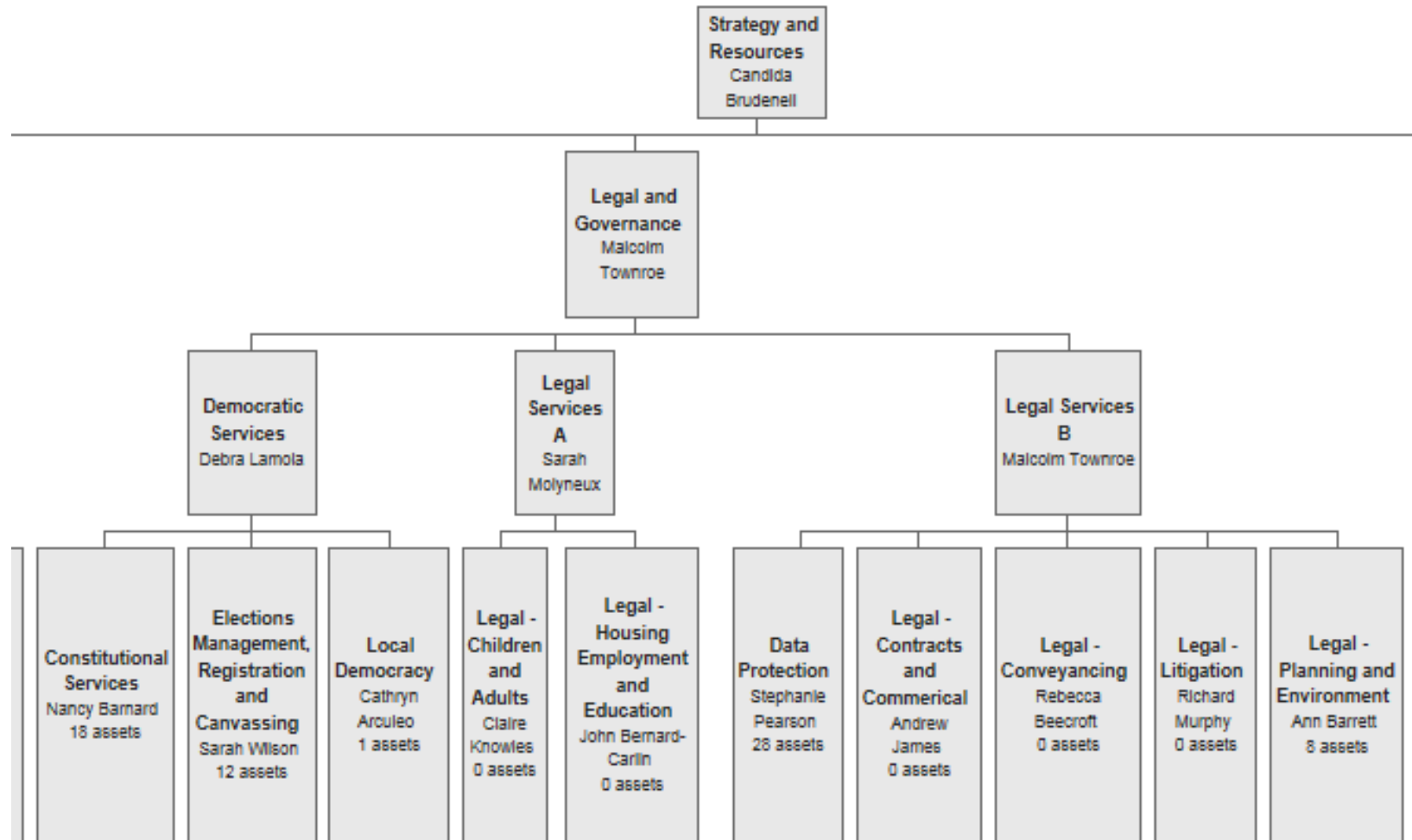
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

- Spreadsheet to carry out Data flow mapping is currently being developed by the DP team/ RM team
- The template will need to be populated by each department in the council – a huge task!
- The Information Asset Register should hold this information, the legal basis of processing and any linked privacy notice, PIA and ISA = records of processing

Organisational charts

Strategy and Resources

ONLY Business Functions which have been assigned a Service Area can be included in this chart.

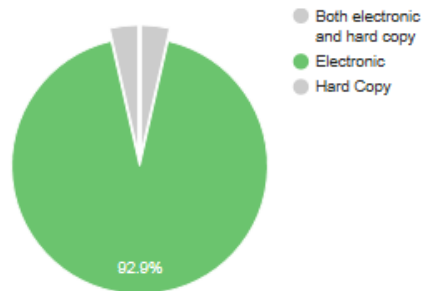


Data Protection

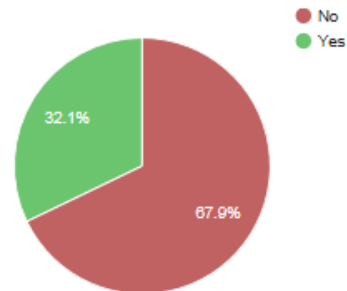
Filtered by Business Function - 28 results.

[Back](#) [Export to Excel...](#)

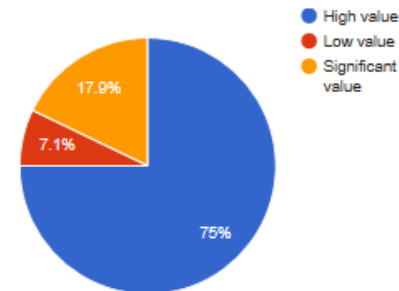
Resource format



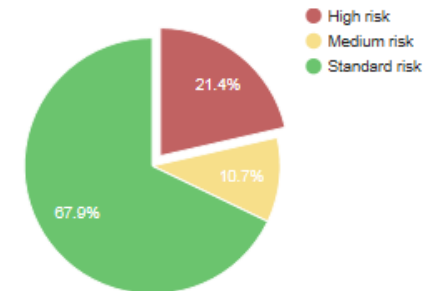
Personal information



Relative value



Risk factor



| ID | Name | Description | IA Manager | PI? | Retention period | Business function | Combined risk | |
|-----|---|---|-------------------|-----|------------------|---|------------------------------|-------------------------|
| 157 | Body Worn Video (BWV) surveillance system guidance | Community Protection Officer's Guidance notes on Body Worn Video (BWV) surveilla... | Stephanie Pearson | No | 0 years ... | Data Protection Strategy and Resources » Legal and Governance » Legal Services B | Business: 3 Individual: 0 | Details |
| 158 | Data Protection - The Act, Policy and Practice guidance | Summary of how the Data Protection Act affects colleagues, and what to do if a d... | Stephanie Pearson | No | 0 years ... | Data Protection Strategy and Resources » Legal and Governance » Legal Services B | Business: 5 Individual: 0 | Details |
| 161 | Personal data requests handling guidance for frontline | Guidance on how to handle requests for personal data. This | Stephanie Pearson | No | | Data Protection Strategy and Resources » | Business: 4 Individual: 1 | Details |

GDPR- Privacy Information

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.

- All consent forms throughout the Council have privacy notices that will need to be reviewed
- There is also a privacy notice on the main intranet that was agreed by Legal Counsel but will be out of date by next May

GDPR Individual rights

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.

- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object



GDPR Subject Access Request

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.

- Subject Access procedure is changing.
- No fee
- They will need to be provided with more information including extra rights, retention period, purposes of processing, how to lodge a complaint etc.
- Times have been reduced for compliance of standard SARs making compliance targets more difficult



Subjects rights under GDPR



- Right to access personal information- Personal information requests (PIR's)
- Once the information audit is completed DP team will be in a position to provide the personal information and the information required to be given by A 15



GDPR Purpose of processing

6

Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

There are many reasons for processing data.

- Consent is one way.
- Others include: Contractual purpose, Legal obligation, statutory power. These gateways are changing for Local Authorities.
- New gateway – Public duty



GDPR Purpose of processing

6

Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

6 Principles (Article 5)

1. Personal data shall be:

- a) Fair, lawful and transparent
- b) Specific, explicit, legitimate purposes
- c) Adequate, relevant, necessary
- d) Accurate, where necessary up to date
- e) Retention
- f) Security



GDPR Purpose of processing

Lawfulness of processing *(Article 6)*

1. One of the following

- a) Consent
- b) Performance of contract
- c) Legal obligation
- d) Vital interests
- e) Public interest/ exercise of Authority
- f) Legitimate interest (not for local Authorities and most schools)



GDPR Purpose of processing

Special Data (*Article 9*)

2. a) Explicit consent
- b) Employment/ social security/ social protection obligations
- c) Vital interests
- d) Non-profit bodies
- e) Processing made public by data subject
- f) Legal claims
- g) Substantial public interest
- h) Health, social care, medicine
- i) Public interest for public health
- j) Archiving, statistics, historical research



GDPR Purpose of processing

Adhere to
6 principles in
Article 5

Select gateway
from
Article 6

For **special
data**
select gateway
from
Article 9

= **Lawful
processing**



GDPR Consent

7

Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

- Many consent forms will need reviewing
- Systems will need to identify whether consent is a reason for processing
- No pre ticked boxes
- Must opt in not opt out



Lawful basis of processing



- Where processing is based on consent must be explicit
- However ICO draft guidance on consent notes that the main basis the local Authorities will use to process data is public task/ public interest
- This will be a big culture change for parts of the Council



GDPR Children's rights

8

Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

- We are still waiting for UK to verify what age children will be required to give consent
- Parts of the council may need to obtain both children and adults consent to process their children's data.
- More rights for children under the GDPR



GDPR Data Breaches

9

Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.



A situation or incident that results in, or has the potential to result in, a breach of one or more of the data protection principles.

- Data breaches will need to be notified to the ICO within 72 hours
- Not all breaches will need to be notified to the ICO

Greater Manchester Police

The following is an example of a data protection breach involving lost post.



You are here → [News](#)

UKA correspondent

Friday 5 May 2017

[in Share](#)

[f Share](#)

[t Share](#)

ICO hits Manchester Police with £150,000 fine

Information commissioner sanctions force for losing unencrypted DVDs of victim interviews

The Information Commissioner's Office (ICO) has hit Greater Manchester Police (GMP) with a £150,000 fine for losing three DVDs containing footage of interviews with victims of violent or sexual crimes.



The force sent the unencrypted DVDs, which showed named victims talking openly, to the Serious Crime Analysis Section (SCAS) of the National Crime Agency in the post by recorded delivery but they were never received. The DVDs have never been found.

An investigation by the Information Commissioner's Office (ICO) found that the police force failed to keep highly sensitive personal information in its care secure and did not have appropriate measures in place to guard against accidental loss. This is a breach of data protection law.



Basildon Borough Council

The following is an example of a data protection breach involving information posted on a planning portal.



Security

30

UK council fined £150k for publishing traveller family's personal data

Medical details exposed in online planning application

By [Kat Hall](#) 31 May 2017 at 15:08

SHARE ▼

An Essex council has been fined £150,000 for publishing highly sensitive personal data, including medical information, of a traveller family via online planning documents.

The Information Commissioner's Office (ICO) slapped Basildon Borough Council for publishing the information in planning application documents, which it made publicly available online for nearly two months.

The council published a full statement containing sensitive personal data relating to a static traveller family who had been living on the site for many years. It referred to the family's disability requirements, including mental health issues, the names of all the family members, their ages and the location of their home.

The ICO's investigation found that on 16 July, 2015, the council received a written statement in support of a householder's planning application for proposed works in a green-belt area. The information was only removed on 4 September when the concerns came to light.



Case Study – Stoke on Trent City Council

The following is a physical loss of a Child's personal information



ICO hits Stoke-on-Trent City Council with £120,000 fine



Jennifer Scott
TechTarget
26 Oct 2012 11:26



Stoke City Council has breached the Data Protection Act, for the second time in two years, after details of a child protection legal case were emailed to the wrong person.

Stoke-on-Trent City Council has been fined £120,000 by the Information Commissioner's Office (ICO) for breaching the Data Protection Act.

A solicitor that worked within the organisation was found to have sent 11 emails containing information about a child protection law suit to the wrong person, which the ICO considered a "serious breach"



GDPR- Privacy by design

10

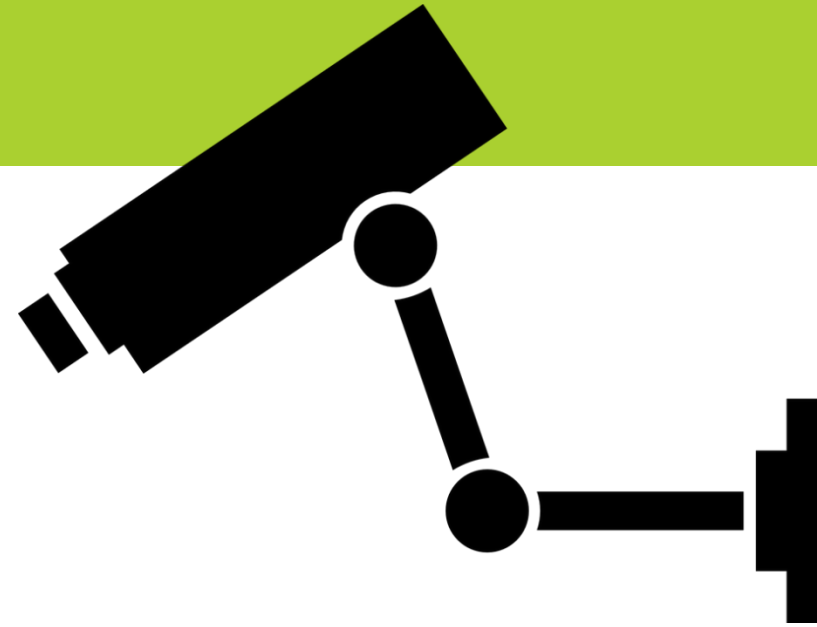
Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

- Where a new type of processing/project takes place using new technologies where there is a high risk to privacy a privacy impact assessment **must** be carried out
- Assessment must look at necessity and proportionality
- Needs to be embedded in process



Data Protection Impact Assessments- DPIA (formerly PIA)



- CCTV
- Body worn Cameras
- Camera in cars/Outside cars
- New APPs that collect lots of sensitive data
- New systems such as liquid logic, Case management systems



GDPR Data Protection Officers

11

Data Protection Officers

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



- Under Article 37 a Data Protection Officer must be appointed where processing is carried out by a public authority. The Data protection officer has to report to the highest management
- Must have expert knowledge of data protection
- Cannot undertake tasks that could create a conflict of interest



GDPR International

12

International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

- Any information held on cloud systems outside the EU
- Contracts with companies in Non EU countries
- Correspondence with citizens / relatives abroad

