General Data Protection Regulation Managers Workshop

March/April/May 2018

Simon Hobbs, Deputy Director of Legal Services and Council Data Protection Officer,
Elizabeth Wild, Principal Solicitor
Martin Stone, Programme Manager - GDPR

Purpose of session

- ✓ What do you need to know about GDPR?
- ✓ What has changed/will change in DCC?
- ✓ What do you need to do differently in the future?

Timetable

1.	Arrival and registration	15 Minutes
2.	Introductions/Housekeeping	5 Minutes
3.	What do I need to know about GDPR?	45 Minutes
4.	Breakout session	30 Minutes
5.	Coffee break	20 Minutes
6.	Changes and Differences due to GDPR?	45 Minutes
7.	Questions	20 Minutes

Housekeeping

- Fire alarm.
- Toilets & facilities.
- Breaks.
- Mobile phones.
- Feedback forms

Accountability is Critical

“ Accountability is at the centre of all this: of getting it right today, getting it right in May 2018 and getting it right beyond that.”

Elizabeth Denham – Information Commissioner.

What do I need to know about GDPR?

Evolution not revolution

GDPR v Data Protection Bill

- GDPR enforceable across EU member states.
- Still applicable after Brexit.
- Includes opportunities to make ‘local’ provisions.
- DPB will update the Data Protection Act 1998 with new Act.
- Covers processing which does not fall within EU law e.g. National Security.
- Comes into force 25th May

Officer roles

Caldicott Guardian

- The Caldicott Guardian should act as the conscience of the organisation, ensuring that both legal and ethical considerations are taken into account, particularly when deciding whether to share confidential information.

Senior Information Risk Owner (SIRO)

- take the lead on delivering risk management and security strategy in the Council and assist Corporate Management Team (CMT) in the delivery of this including chairing the Information Governance Group (IGG)

Data Protection Officer (DPO)

- Accountable to the Council via Corporate Management Team to monitor compliance with GDPR. First point of contact for ICO etc.

What is Personal Data?

Means any information relating to an identified or identifiable living person ('data subject')

Is this personal data?

- Name
- IP Address
- Eye colour
- Payroll Number
- E Mail Address
- Biometric Data

General Data Protection Regulation (GDPR)

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. **Lawful basis for processing personal data**
   You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.
7. **Consent**
   You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
8. **Children**
   You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any 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 ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.
11. **Data Protection Officers**
    You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.
12. **International**
    If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico. Information Commissioner's Office

ico.org.uk

Key Changes (1)

- Applies to controllers (DCC) and processor (provider)- retrospective as to contracts
- Lawful basis for processing -more focussed attention- special categories need to meet additional safeguards.
- Transparency- privacy notices.
- Data Sharing; must be written agreement
- Breach notification- more onerous.
- Enforcement and higher compensation potential

Article 5 - Key principles

Personal data must be:

- Processed lawfully
- Collected for specific explicit and legitimate purpose
- Adequate, relevant and limited to what is necessary
- Accurate and up to date
- Kept only for as long as necessary
- Kept secure

NB Consent is not always required

Article 9 – Special Categories of Data

Special Categories of Personal Data" rather than Sensitive Personal Data.

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs, or
- Trade union membership, and
- The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
- Data concerning health, or
- Data concerning a natural person's sex life or sexual orientation.

Lawful processing

- **Consent:** an individual has given clear consent for you to process their personal data for a specific purpose
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal Obligation:** the processing is necessary for you to comply with the law (not including contractual obligations)
- **Vital Interests:** the processing is necessary to protect someone's life.
- **Public Task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate Interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party (this cannot apply if you are a public authority processing data to perform your official tasks).

Necessity

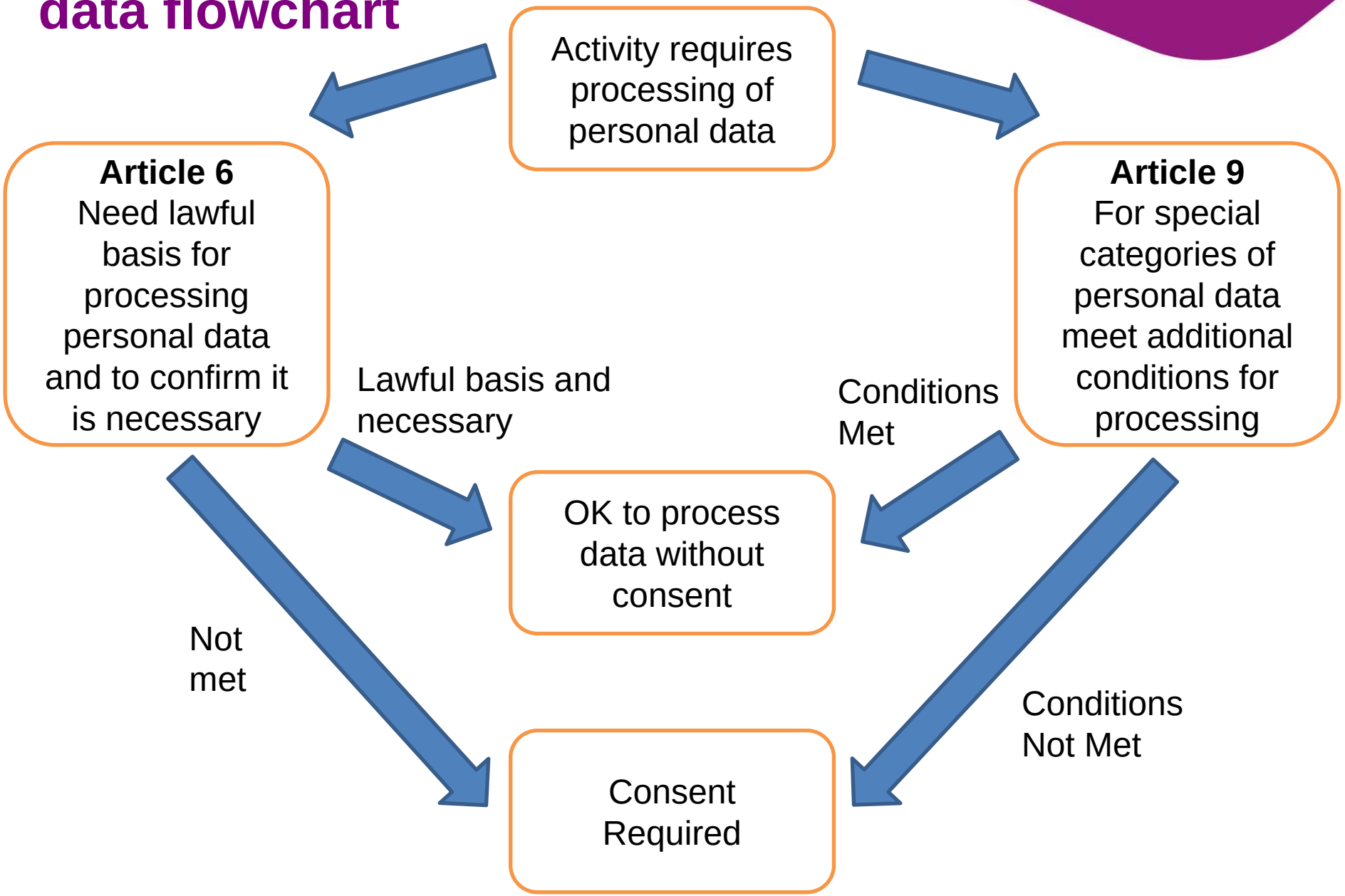
- You need to decide which reason for lawful processing is appropriate and (except for consent) whether it is necessary
- Many of the lawful bases for processing depend on the processing being “necessary”.
-
- This does not mean that the processing has to be essential, but it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other, less intrusive means.
- The question is whether the processing is necessary for the stated purpose, not whether it is a necessary part of your method of pursuing that purpose.
- **If you are not sure then take advice**

Conditions for processing special categories of data

- Additional conditions apply to processing special categories of personal data

- Take advice when processing this type of data as consent may well be required

Lawful basis for processing data flowchart



Key changes (2) - Individuals' rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making and profiling

Right to be Informed (1)

Privacy Notices

- The right to be informed encompasses the obligation on the controller to provide fair processing information, usually through a privacy notice
- The aim is to ensure transparency over how personal data is used
- Information supplied about processing must be:
  - Concise, transparent, easily accessible
  - Written in clear, plain language
  - Free of charge

Right to be Informed (2)

- Information which must be supplied in a privacy notice:
  - Identity and contact details of the controller and the data protection officer
  - Purpose of the processing and the lawful basis for the processing
  - The legitimate interests of the controller or third party, where applicable
  - Categories of personal data
  - Any recipient or categories of recipients of the personal data
  - Details of transfers to third country and safeguards
  - Retention period
  - The existence of the data subject's rights
  - The right to withdraw consent, where relevant
  - The right to lodge a complaint with the supervisory authority
  - The source the personal data originates from and whether it came from publicly accessible sources
  - Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
  - The existence of automated decision making

The Right of Access

- Individuals have the right to access their personal data and supplementary information
- A copy must be provided free of charge
- Information must be provided within one month.
- Information should be provided in accordance with the Council's 'Subject Access Request (SAR) Procedure'

Right to Erasure

- Also known as the right to be forgotten.

- Generally an individual does have a right to request deletion of their personal data UNLESS there is a compelling reason for it not to be deleted.

Examples of compelling reasons are:

- to comply with a legal obligation for the performance of a public interest task or exercising official authority
- the exercise or defence of legal claims

Children

- Require particular protection as they are less aware of the risks involved
- Still require a lawful basis for processing
- Consent: if consent is required:
  - (a) the child must be aged 13 years or over (this is the age currently stipulated in the Data Protection Bill) in order to be considered able to give consent themselves;
  - (b) for those under 13 years, consent from those who have parental responsibility is required – unless you are providing a preventative or counselling service
- A clear privacy notice in clear age-appropriate wording must be in place
- Have the same rights as adults in relation to their information, but some, for example, the right to erasure, may be particularly relevant

Group Exercise

Read through the example Privacy Notice on your table and identify what are its good points and what are its bad points?

Group Exercise – Points to Consider

- Lacks proper title and identity or contact details (DPO)
- Overly legalistic and complicated
- Does not explain individual rights adequately
- Nothing about withdrawal of consent
- Details about access to records right in small print and inaccurate
- No link to main Council privacy notice web page
- Good explanation of why telephone contact needed
- Did identify specific purpose of data processing

What has changed/will change in DCC ?

An evolving picture

Progress to date (1)

- GDPR Workshops for managers in progress
- New GDPR on line training available on Derbyshire LearningPool on line training system
- Data Protection by Design -Privacy Impact Assessment process established for new projects and data sharing; 8 workshops on PIA's for staff currently under way
- Section of website on GDPR established and being added to with information and guidance
- Initial publicity to staff via Our Derbyshire and Members Bulletin

Progress to date (2)

- DPO identified- senior roles appointed to and defined
- Council Data Protection Policy approved
- Contracts register established. Contractual changes consequent on GDPR; guidance and template letters published
- Register of data sharing agreements being drawn up
- Information Audits across Council largely completed and project group formed to review compliance with GDPR requirements

Progress to date (3)

Information audits review- emerging issues

1. Is legal basis for processing personal data known?
2. Are special categories of personal data being processed?
3. Is there a GDPR compliant consent process in place (if applicable)?
4. Has 3rd party supplier contract been updated where personal data is being processed (if applicable)?
5. Is data sharing agreement in place for sharing personal data (if applicable)?
6. Has departmental Privacy Notice been updated (if applicable)?
7. Is the retention period stated for the personal data held recorded on the departmental retention schedule?
8. Is the location of the personal data known?
9. Can system or process handle requests relating to individuals' rights under GDPR and delete records in line with record retention schedules?
10. Is there appropriate security in place for personal data?

Other work in progress

- Review of policies/procedures, consent and privacy notices
- Review of lawful basis for processing (following audits)
- Subject access requests- revised timescales; development of EDRM
- Complaints process being revised to take account of GDPR complaints
- Breach following unauthorised disclosure ; procedure being established
- Training and awareness; Communication plan to embed this
- Compliance- KPIs being developed
- ICT strategy to include GDPR compliance and general data management policy to be developed.

What will I need to do differently in future?

Taking personal responsibility for data protection

Policies and procedures

Familiarise yourself and your staff with new policies and procedures

For example;

SAR's – new timescale one month unless complex

Privacy Impact Assessments

3rd Party relationships with suppliers and providers

- Take responsibility for data protection and confidentiality …ditch the data demon
- Make sure you and your staff have completed the on line IG training

Awareness of individual rights and how to apply these

Before commencing on a new project or data sharing agreement:

1. Consider whether a Privacy Impact Assessment is required
   - information privacy is the ability of an individual to control information about themselves
   - systematic process to identify privacy risks (ie. risk of harm arising through the processing of data) of a project and mitigate them

2. Identify the basis for processing and ensure that it is lawful
   - Complete privacy notice
   - If required, ensure appropriate consent is obtained

3. Rights of access
   - Ensure you are aware of the SAR (Subject Access Request Procedure)

Data Sharing Agreements

- Whenever information is shared, the GDPR requires there to be a Data Sharing Agreement in place. This includes:
  - Data sharing between controllers
  - Sharing data between a controller and a processer
  - Sharing data between a processor and sub-processor
- Data sharing agreement register is being established, template for new agreements and guidance to follow

Contracts with Third Parties

- Where third parties are involved, i.e. a processor who processes personal data on behalf of the controller, there must be a written contract in place

- This is to ensure that both the controller and the processor understand their obligations, responsibilities and liabilities to assist them to comply with the GDPR and help controllers to demonstrate compliance with GDPR

- Recommended clauses and associated correspondence are available on DCC website

Third Party Due Diligence

- Controllers (i.e. DCC) will need to have in place technical and organisational security measures to ensure that third parties are meeting their responsibilities and should look at:
  - Pseudonymisation and encryption
  - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
  - The ability to restore the availability and access to the personal data in a timely manner in the event of physical or technical incident
  - The process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

Data Breaches

Impact:

- Significant harm to individual e.g. physical, financial or damage to reputation
- Damage to reputation of Council e.g. loss of trust
- Compensation claims from individuals
- ICO financial penalties

Avoiding Data Breaches

- Lock PC
- Don’t transfer personal data to other agencies without checking
- Don’t keep information for longer than needed
- Don’t leave files in car, keep then secure at home
- Check email address
- Use encrypted e mail

Reporting Data Breaches

- Inform line manager
- Record on Service Desk Online – Security Incident Form
- Investigate
- Mitigate impact as soon as possible
- Put in place measures to prevent repeat incident
- Some breaches may need reporting within 72 hours to ICO, take legal advice as soon as possible

Members' registration

- All Members were registered as data controllers following election in May 2017
- Council is also registered
- Members' Case Management System has been subject to Information Audit process
- Likely that registrations will be required after May; ICO is to clarify;
- Uncertain whether the requirement to be registered as Data Controller would still stand under the GDPR. Bill is still before Parliament – 'once the procedure for registration has been finalised, Data Controllers would receive an email clarifying the position.'

Contacts

GDPR Preparation Group

- Simon Hobbs DPO
- David Gurney (AC)
- Christine Hampshire (CCP - IT)
- Jane Morgan (CCP - Non IT)
- Chris Newton (CS)
- Angela Glithero (ETE)
- Martin Stone Programme Manager - GDPR

Queries about GDPR:
Go to www.derbyshire.gov.uk/gdpr
or email gdpr@derbyshire.gov.uk

Any Questions?

Thank you and we would be grateful if you could complete the on line evaluation form for this workshop at

https://www.snapsurveys.com/wh/s.asp?k=146347666353

Copies of this presentation can be found at:

www.derbyshire.gov.uk/gdpr