General Data Protection Regulation Workshop for DCC Providers

May/June 2018

Martin Stone, Programme Manager - GDPR

Workshop Agenda

- ✓ What do I need to know about GDPR?
- ✓ What is the impact of GDPR on my relationship with Derbyshire County Council?
- ✓ GDPR and data security

Housekeeping

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

What do I need to know about GDPR?

GDPR v Data Protection Bill

- GDPR enforceable across EU member states.
- Still applicable after Brexit.
- Includes opportunities to make ‘local’ provisions.
- A new UK Data Protection bill 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

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

Data Controller

Data controller means … 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.

- Put simply, if you collect and store personal information you are likely to be a data controller

Data Processor

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

- Put simply, if you deal with or store data on behalf of another party you are likely to be a data processor.

Key Changes (1)

- Applies to controllers (e.g. 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

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).

Conditions for processing special categories of data

- Special category data is personal data which the GDPR says is more sensitive and so needs more protection.

- Therefore, processing of this type of data is prohibited unless one of the conditions specified in Article 9 (to be covered in Schedule 1 of the DPA 2018) applies in addition to establishing a lawful basis for processing the data.

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.

Key changes - 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

What is the impact of GDPR on my relationship with Derbyshire County Council?

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

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

Obligations of Provider when acting as Data Processor for Council personal data

- To protect the rights of the data subject
- Not to use the data for any other purpose
- To act in accordance with any instructions from the Council relating to the data
- To ensure confidentiality is maintained
- Return or delete the data at the end of the contract
- To keep the data secure
- Report data breaches as soon as possible

Third Party Due Diligence

Controllers (e.g. 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.

GDPR and Data Security?

Taking personal responsibility for data protection

Data Breaches

Impact:

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

Avoiding Data Breaches

- 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
- Don’t hold conversations about a customer/client in a place where they will be overheard
- Don’t discuss personal details of customers/clients at home, in the pub or on social media
- Check email address
- Use encrypted e mail
- Lock PC when not using it

Practical Steps – Paper Records

- Paper records containing personal data should be locked away at the end of each working day.
- Keys used to keep information secure should only be provided to individuals who need them.
- Personal data should be shredded when no longer required.
- Personal data should not be left on printers, faxes, photocopiers.
- When transporting personal data by a vehicle, all records must be held securely when left unattended.

Practical Steps – Electronic Records

- Personal data sent electronically including spreadsheets, letters and schedules should be password protected.
- Personal data should only be sent by fax where no other options are available.
- Personal data should be deleted when no longer required.
- Personal data should not be published on social media.
- Personal data should not be sent via text or instant messaging services.

Practical Steps - Smartphones & Tablets

- Switch on password and PIN protection (Do not use 123456!).
- Make sure lost or stolen devices can be tracked, locked or wiped.
- Keep your device up to date.
- Keep your apps up to date.
- Don't connect to unknown Wi-Fi Hotspots.

Practical Steps - Backing up your data

- Identify what data you need to back up.
- Keep your backup separate from your computer.
- Consider the cloud.
- Make backing up part of your everyday business.
- Keep your backups secure.

Practical Steps – Viruses & Malware

- Install (and turn on) antivirus software.
- Don’t download dodgy apps.
- Keep all your IT equipment up to date (patching).
- Control how USB drives (and memory cards) can be used.
- Switch on your firewall.

Practical Steps – Avoid being Scammed

- Avoid using predictable passwords.
- Change all default passwords.
- Consider encryption.
- Check your digital footprint.

Reporting Data Breaches

- Inform Council as soon as possible
- Record Incident
- Investigate
- Reduce 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

Getting in Touch

If you have any questions relating to GDPR and your contract with Derbyshire County Council the contacts are a follows:

For Adult Care contracts:

Teresa.Whetton@derbyshire.gov.uk

For Transport related contracts:

Deborah.Oddy@derbyshire.gov.uk

Any other GDPR related questions in relation to Derbyshire County Council e mail

GDPR@derbyshire.gov.uk

Useful Resources

- ✓ Information Commissioner's Office guidance for small business

https://ico.org.uk/for-organisations/business/

- ✓ Cyber Security: Small Business Guide

https://www.ncsc.gov.uk/blog-post/cyber-security-small-business-guide

- ✓ General advice on GDPR in relation to Derbyshire County Council

www.derbyshire.gov.uk/gdpr

Thank you for listening

Any Questions?

Copies of this presentation can be found at:

www.derbyshire.gov.uk/gdpr