Briefing for Audit Committee Members on the General Data Protection Regulation

February 2018

Simon Hobbs, Deputy Director of Legal Services and Council Data Protection Officer,

Elizabeth Wild, Principal Solicitor

Purpose of session

- ✓ Provide overview of the General Data Protection Regulation (GDPR) and Data Protection Bill (DPB), effective 25th May 2018
- ✓ Set out DCC governance and our progress against ICO ‘12 steps’
- ✓ Impact on Members
- ✓ Training and communications

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.

DCC Governance

- Cabinet
- Audit Committee
- Corporate Management Team
- Information Governance Group (IGG)
- GDPR Task and Finish Group established Summer 2017 and GDPR Programme Plan finalised January 2018
- Caldicott Guardian- Joy Hollister
- SIRO/Chair IGG- Peter Handford
- DPO- Simon Hobbs
- Programme Manager GDPR- Martin Stone

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.

ICO Audit September 2017

(1) Governance
(2) Subject Access Requests and
(3) Privacy Impact Assessments

- Graded yellow overall- reasonable level of assurance that processes and procedures are in place and delivering data protection compliance- summary of inspection published by ICO

https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2172529/dcc-audit-summary-20170922.pdf

- ICO action plan monitored via IGG

Current Position

Good record of compliance with current DPA 1998 legislation

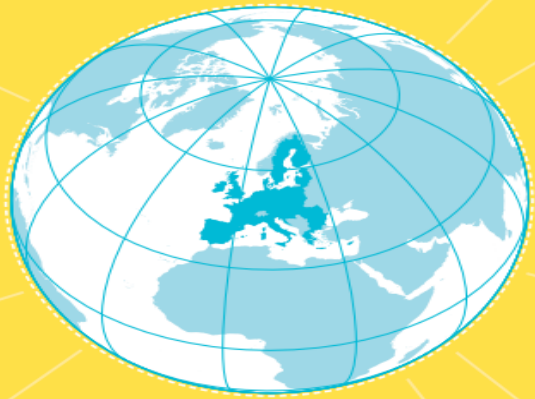
Information security policies and procedures already in place with ISO27001 certification

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.
- Updates ‘local’ provisions.
- Covers processing which does not fall within EU law e.g. National Security.

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

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

What is Personal Data?

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

- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- IP address or roll number can amount to personal 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.

Progress to date (1)

- DPO identified- senior roles appointed to and defined
- Council Data Protection Policy approved
- Workshops for staff
- Information Audit across Council largely completed project group formed to check legal basis and ability to comply with GDPR requirements
- Section of website on GDPR established and being added to with information and guidance-

https://www.derbyshire.gov.uk/working_for_us/data/gdpr/default.asp

Progress to date (2)

- Data Protection by design -Privacy Impact process established for new projects and data sharing; 8 workshops for staff currently under way
- Contracts register established. Contractual changes consequent on GDPR; guidance and template letters published
- Register of data sharing agreements being drawn up
- New GDPR on line training on Learning Pool imminent
- Awareness- initial publicity to staff via Our Derbyshire and Members Bulletin.
- Further workshops planned for March/April for staff and Members

WIP as per plan

- Review of policies/procedures, consent and privacy notices
- Subject access requests- revised timescales; 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

GDPR noted on Corporate Risk Register

Risk of noncompliance with new data protection legislation effective from May 2018. Increased level of scrutiny and larger potential fines.

Impact 4 Probability 3 Total 12

Risk mitigation- IGG has oversight. Working group established Summer 2017 and action plan in place. ICO audit in September 2017 found adequate arrangements in place. Data Information Audit largely completed. Privacy Impact Assessment process embedded in procurement and data sharing projects. Training of staff managing data undertaken.

Planned mitigation; further training and increased level of communications, review of policies and procedures. Contract variation with suppliers. Deletion of personal data is potential area of challenge for Council and may have to be approached on a functional basis

Target mitigated score Impact 4 Probability 2 Total 8

Impact of Breaches

- 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 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 them secure at home
- Check email address
- Use encrypted e mail

Examples of Breaches in Past

Scottish Borders Council - former employees' pension records were found in an over-filled paper recycle bank in a supermarket car park - were fined £250,000

Greater Manchester Police - after the theft of an unencrypted memory stick containing sensitive personal data from an officer's home - were fined £150,000

Devon County Council - social worker used a previous case as a template for an adoption panel report left in identifiable details relating to previous report – were fined £90,000

London Borough of Lewisham - after a social worker left sensitive documents in a plastic shopping bag on a train, after taking them home to work – were fined £70,000

The potential penalties under the new regulation are significantly greater.

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 be required after May
- But 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.'

Training

- On line training- on Learning Pool
- Additional workshops- provisional dates

5th March AM

14th March PM

9th April AM

16th April PM

Would these be useful for Members to attend?

Questions?

GDPR.mailbox@derbyshire.gov.uk