South Lakeland District Council

Audit Committee

Wednesday, 5 December 2018

Implementation of General Data Protection Regulations and Data Protection Act 2018

Portfolio:	Councillor Jonathan Brook, - Housing, People and Innovation Portfolio Holder
Report from:	Debbie Storr, - Director of Policy and Resources (Monitoring Officer)
Report Author:	Paul Mountford, - Principal Performance and Intelligence Officer
Wards:	Not Applicable
Forward Plan:	Not applicable

1.0 Expected Outcome

1.1 This report sets out the work undertaken to implement the General Data Protection Regulation and Data Protection Act 2018 across the Council.

2.0 Recommendation

2.1 It is recommended that the Audit Committee notes the update on the introduction of the General Data Protection Regulation and Data Protection Act 2018 across the Council and provides any comments.

3.0 Background and Proposals

3.1 The Data Protection Act 2018 (DPA) covers the use of personal data within the scope of the General Data Protection Regulation (GDPR) and beyond it. Amongst other provisions, it repeals and replaces the Data Protection Act 1998, incorporates the GDPR into UK law, lays the ground for free-flow of data between the United Kingdom and the European Union after Brexit, sets out permitted exemptions under the GDPR and sets out the duties and powers of the UK's Information Commissioner's Office (ICO).

3.2 With administrative fines under the new DPA now having an upper limit of 20 million Euros, it is crucial that the Council is compliant with the GDPR/ DPA, as it has been under the Data Protection Act 1998. This report sets out the work undertaken to prepare for and implement GDPR across the Council.

3.3 The General Data Protection Regulations Project Initiation Document was presented to Audit Committee on 6 December 2017. This set out the scope, objectives, outcomes and deliverables of the project.

3.4 The Information Governance Board, as outlined in the General Data Protection Regulations Project Initiation Document, has been established to ensure senior leadership, drive and accountability.

3.5 The current Principal Performance and Intelligence Officer has been appointed as the Council's Organisational Data Protection Officer. The Principal Performance and Intelligence Officer has qualified as a General Data Protection Regulation Practitioner.

3.6 A number of activities are in operation to ensure continued compliance with the law:

- **E-Learning** - A GDPR e-learning package has been developed and made mandatory for all officers. The Data Protection Officer is monitoring the training records with the Learning and Development Team.
- **Non IT Workers** - Operatives with no access to IT will be offered workshops in February 2019 to provide GDPR training bespoke to their particular needs.
- **Members** – The Data Protection Officer delivered DPA/GDPR training to Members in March 2018. Further dates in early 2019 will be offered to all new and established Members.
- **SharePoint** – A dedicated Data Protection SharePoint has been posted on the Council's Intranet.
- **Town/Parish Councils** - Training workshops, in partnership with the Cumbria Association of Local Council's (CALC), for Clerks and Members of Town and Parish Councils is scheduled for the spring of 2019 emphasising the requirements for the completion of Information Asset Registers, Privacy Notices and Data Protection Impact Assessments.
- **Partners** – Partner organisations are individually responsible for the application of the DPA and it is the Council's responsibility to gather assurance/evidence that such organisations are implementing the law correctly. Where any contractual arrangements exist with partners, we include requirements for them to be compliant with GDPR/DPA 2018.

3.7 A number of documents have been formally reviewed by Management Team and/or Cabinet (where appropriate) to assist Members, Officers, and members of the public. These include (not exhaustive list):

- Data Protection Policy
- Retention Policy
- Information Management Policy
- Information Security Policy
- Data Quality Policy
- Personal Data Breaches Guidance
- Privacy Notices
- Acceptable Use Policy
- Subject Access Request Form
- Data Protection Impact Assessment (DPIA) Guidance
- Information Asset Register (IAR)

3.8 The Council's Information Asset Register is complete and has been published on the Council's SharePoint. The Council's Register of Processing Activity, in accordance with Article 30 of the GDPR is complete and is published on the Council's dedicated Data Protection SharePoint.

3.9 An Information Asset Register (IAR) is a simple way to help the Council understand and manage its information assets and the risks to them. It is important to know and fully understand what information the Council holds in order to protect it.

3.10 In support of the Council's IAR, the Information Handling and Classification Protocol is in place and will be applied in accordance with the overall GDPR/DPA 2018 implementation.

3.11 A generic corporate Privacy Notice has been published on the Council's website covering all services provided by the Councils. Alongside this Privacy Notice, service specific Privacy Notices for every service are being added. Privacy Notices advise our customers what information about them is collected, when it is collected, how it is used, how long it is kept and whether it is shared, and with whom. The Notices also set out peoples' rights under GDPR and DPA 2018. Publication of Privacy Notices is an ongoing task, and the Notices published to date can be found on the Council's website.

3.12 A Data Protection Impact Assessment (DPIA) must be performed where processing is likely to result in a high risk to the rights and freedoms of natural persons. Where the Information Asset Registers have identified that the Council is holding sensitive data (for example ethnic origin, religion, health data), a DPIA will need to be completed to risk assess such data and ensure it is held as securely as possible.

3.13 A template Data Processing Agreement has been implemented and shared with Procurement Services which will accompany all procurement documents where it is considered relevant.

3.14 A Data Breach Notification Protocol is in place and is available to all Officers through the dedicated Data Protection SharePoint.

3.15 A procedure for implementing the Subject Access process is in place. The amended Subject Access Request form is available to the public via the Council's website.

4.0 Consultation

4.1 The Data Protection Officer continues to provide regular updates to Corporate Management Team and Operational Managers. This report updates Members on the work undertaken on the implementation of GDPR and the Data Protection Act 2018.

4.2 The internal audit work programme for 2018/19 includes a review of information governance across the Council and this will consider the management of information in accordance with GDPR. This audit is due to commence in the New Year and will be reported back at some future date.

5.0 Alternative Options

5.1 As the Council is already compliant with the requirements of the Data Protection Act 1998, it is in a positive position to adapt to the enhanced obligations of the General Data Protection Regulation and Data Protection Act 2018.

6.0 Links to Council Priorities

6.1 The General Data Protection Regulation and Data Protection Act 2018 forms part of the overall Information Governance Framework. The framework links directly to the Council Plan 2014 -2019, under the strategy heading of Innovation - as it will improve customer service and access to Council services.

7.0 Implications

Financial, Resources and Procurement

7.1.1 At present there is no dedicated budget required for the work to support implementation of the General Data Protection Regulation. The Principal Performance and Intelligence Officer, as Data Protection Officer, is continuing to monitor the deliverability of the actions within existing resources.

7.1.2 The current resource assessment is that implementation should be managed within existing budgets. This is consistent with the approach taken by other authorities at this stage, however the scale and potential cost of changes remains unknown and therefore difficult to quantify with any certainty. There are two potential areas of concern that will be closely monitored:

- the financial impact of variance to contracts or processor agreements to ensure they are compliant with the General Data Protection Regulation; and,
- changes to the council's ICT Infrastructure to ensure security requirements and individual rights can be met.

7.1.3 If the Council fails to notify a breach to the Information Commissioner's Office within the 72 hour period or if the Council fails to comply with any aspect of the General Data Protection Regulation then the Council could be facing significant fines of up to €10 million or 2% of total worldwide annual turnover (whichever is the greatest) for level 1 fines, and fines of up to €20 million or 4% of total worldwide annual turnover (whichever is the greatest) for level 2 fines.

Human Resources

7.2.1 The implications for the Council are significant and impact on the working practices of all employees, members and contractors. It is essential that anyone working for the Council (including contractors and partners) who handles personal data is aware of the procedural requirements and responsibilities of the General Data Protection Regulation and Data Protection Act - whether that is responding lawfully to requests, preventing data breaches or proactively adopting privacy by design in everyday working practices.

7.2.2 A lack of preparedness and understanding of the requirements of the General Data Protection Regulation and Data Protection Act may lead to data breaches and enforcement action. Given the scale of the new financial penalties for breaching the General Data Protection Regulation and Data Protection Act principles, this could be costly and also damage the Council's reputation as individuals may lose confidence in the council's ability to safeguard and protect personal data

Legal

7.3.1 The European Union General Data Protection Regulation replaces the Data Protection Directive 95/46/EC and came into force on 25 May 2018. The General Data Protection Regulation is designed to:

- harmonise data privacy laws across Europe;
- protect individual data privacy rights; and
- reshape organisational approaches to data privacy and reduce data breaches.

7.3.2 The Data Protection Act 2018 also came into force on 25 May 2018. The Act:

- establishes a new data protection regime for non-law enforcement data processing, replacing the Data Protection Act 1998;
- ensures the UK data protection framework is suitable for the digital age; and,
- strengthens the rights of, and empowers, individuals to have more control over their personal data including a right to be forgotten when individuals no longer want their data to be processed, provided that there are no legitimate grounds for retaining it.

7.3.3 For a significant period of time prior to the new legislation coming into force, there was a lack of guidance as to the steps organisations could take to ensure compliance. Guidance is now available and the Council has regard to such guidance when implementing its policies and procedures.

Health, Social, Economic and Environmental

7.4 Have you completed a Health, Social, Economic and Environmental Impact Assessment? **No**

7.5 The General Data Protection Regulation and Data Protection Act contains no specific reference to health, social, economic and/ or environmental considerations, so at this stage there are no issues to consider beyond those associated with the current Data Protection Act provisions.

Equality and Diversity

7.6 Have you completed an Equality Impact Analysis? **No**

7.7 The General Data Protection Regulation and Data Protection Act contains no specific reference to equality considerations, so at this stage there are no issues to consider beyond those associated with the current Data Protection Act provisions.

Risk

Risk	Consequence	Controls required
Information Governance Framework, and its policies and guidelines are not fit for purpose.	Distress or harm to individuals or organisations. Reputational damage to the Council. Financial loss or monetary penalty imposed. Detrimental impact on Council business and service delivery. Non-compliance with legislation and potential litigation.	Framework, policies and procedures are to be checked, tested and consulted upon with relevant users.

Contact Officers

Paul Mountford, Principal Performance and Intelligence Officer, 01539 793271, p.mountford@southlakeland.gov.uk

Background Documents Available

Name of Background document	Where it is available
REGULATION (EU) 2016/679	General Data Protection Regulation (EU 2016/679)
Data Protection Act 2018	Data Protection Act 2018
General Data Protection Regulation	SLDC Audit Committee - AUD37
Data Protection Policy and Data Breach Notification Protocol	CEX/10
Information Governance Framework	CEX/63

Tracking Information

Signed off by	Date sent
Legal Services	13 November 2018
Section 151 Officer	13 November 2018
Monitoring Officer	13 November 2018
SMT	13 November 2018

Circulated to	Date sent
Assistant Director	13 November 2018
Human Resources Manager	13 November 2018
Communications Team	N/A
Leader	N/A
Committee Chairman	N/A
Portfolio Holder	20 November 2018
Ward Councillor(s)	N/A
Committee	5 December 2018
Executive (Cabinet)	N/A
Council	N/A