DATA PROTECTION ACT AND GDPR

Cabinet Member for Finance & Democratic Services

Date:	1 May 2018
Agenda Item:	3
Contact Officer:	Bal Nahal
Tel Number:	01543-308002
Email:	bal.nahal@lichfielddc.gov.uk
Key Decision?	**NO**
Local Ward Members	If any Wards are particularly affected insert the name of the Ward Members and their Ward. Ensure that the Ward Members have been consulted.

Lichfield district council
www.lichfielddc.gov.uk

CABINET

1. Executive Summary

1.1 To inform Members of progress made to date in respect of preparing for a change in data protection legislation, known as GDPR (General Data Protection Regulation).

1.2 Members who process data on behalf of constituents whilst doing case work also need to comply with GDPR as they are data processors. The Council ensures that Members are registered with the ICO to undertake these duties.

2. Recommendations

2.1 That Members note the actions to date and the planned measures to ensure compliance with the legislative requirements.

2.2 To appoint Assistant Director Democratic & Regulatory Services at South Staffordshire Council as the Council's Data Protection Officer for 2 years effective from 2 May 2018.

3. Background

3.1 GDPR [the new data protection law] comes in to force on 25 May 2018. It replaces the European 'directive' that the current Data Protection Act 1998 is based on with a 'regulation'. GDPR needs to be read alongside the new Data Protection Bill. This Bill is currently going through the parliamentary process and when it comes in to effect [this must be at the same time as GDPR] it will replace the current Data Protection Act 1998.

The new law must be complied with by the Council as well as members of the Council in their own right as data controllers. Member training is scheduled for Thursday 19 April 2018. At that session members will be advised as to what support they will receive to help them comply with the new law.

Personal data is any information that relates to an identified or identifiable individual.

Data protection is regulated by the Information Commissioner's [Elizabeth Denham] Office.

The Commissioner has described GDPR [for those who currently comply with the law] as an "evolution" not a "revolution". She has also stated that she prefers the "carrot" rather than the "stick" which means that her approach is to encourage organisations to comply in the first instance.

It should be noted however that the new regime does include potentially much more severe penalties for data breaches and increased requirements to notify non-compliance to the ICO.

The ICO's guidance on the steps to be taken can be seen here.

3.2 **Action Taken**

The Council has a project team (consisting of one or more representatives from each service area) led by David Campbell - a Solicitor employed by South Staffordshire Council.

In order to become 'GDPR compliant' the Council needs to take the following steps (following the ICO guidance referred to above):

1. Awareness

Senior Officers and Members should be made aware of the changes under GDPR so that impact and key areas can be identified and managed.

The Council has allocated a significant amount of officer time into preparation work to ensure compliance. Senior Officers have been kept informed throughout and this report will update Members in respect of steps taken and action needed.

2. Information you hold

There is a need to undertake an information audit across the Council and have records of processing activities.

Service teams have identified what personal data the Council processes, who has access, who it is shared with etc. This 'audit' has helped inform the project plan which is being implemented across the Council.

3. Communicating privacy information

Current privacy notes should be reviewed and a plan put in place for making any necessary changes.

This work has been scoped as part of the project plan. There are a number of privacy notices in place across the Council and these are being reviewed and refreshed as necessary to include the lawful basis for processing the data, data retention periods and the right to complain.

4. Individuals' rights

Procedures should be checked and updated to ensure all the rights individuals have are included.

These rights are a mix of refinement of the old and (some) new such as (not exhaustive):

a) The right to access data
b) The right to have incorrect data rectified
c) The right to have data erased [new]
d) The right to data portability [new – but unlikely to be a concern to the council]
e) The right to restrict processing
f) The right to object to processing [limited effect on the council]
g) The right to object to marketing

The Council already has procedures in place to deal with the existing rights; possibly the most significant new right is the right to have data erased. This is not an absolute right and if there is a legitimate business need to retain data then this right can be overridden. However, the Council will need to have an appropriate procedure in place to deal with any such requests. This is being drafted and will be in place in time for May 2018.

5. Subject access requests

Procedures should be updated to allow for the new rules:

- *generally information should be provided free of charge (currently there is a standard £10 charge)*
- *Information should be provided within one month (currently this is 40 days)*
- *If refusing a request for access, we must tell the person why and set out their rights to complain and to judicial remedy; again there is a time limit of one month to do this.*

Whilst the Council does not receive a significant number of subject access requests, procedures and systems are being reviewed to ensure we can comply within the new shorter timescales.

6. Lawful basis for processing data

The lawful basis for processing data must be identified, documented and set out on a privacy notice.

For the Council's statutory functions this will usually be that we are acting in the public interest or exercising official authority. For non-statutory function such as leisure the basis will typically be that the council provides services under a contract.

This is important as the lawful basis impacts on a person's rights under GDPR; if using consent as a basis for processing data then an individual has greater rights to have that data deleted.

Again, officers are working through this in each service team to ensure the lawful basis for processing data is clear and documented.

7. Consent

How we seek, record and manage consent should be reviewed and refreshed as necessary.

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in.

Where the Council relies on consent to process data, the consents given will be reviewed as part of the preparation work and if necessary (this will be on a case by case basis) revised and renewed.

8. Children

GDPR brings in special protection for children's personal data and its use particularly for online services. The need for consent from either the child (if 16 or over) or the parent/guardian is explicit.

9. Data breaches

Procedures should be in place to detect, report and investigate a personal data breach.

Only certain breaches have to be notified to the ICO; where it is likely to result in a risk to the rights and freedoms of individuals e.g. discrimination, damage to reputation, financial loss etc. These breaches should also be notified to the individual concerned.

The Council currently has a procedure in place to deal with data breaches and this is being reviewed to ensure compliance with GDPR requirements. It is not anticipated that any significant changes will be necessary.

10. Data Protection by Design and Data Protection Impact Assessments

It will be a statutory requirement to adopt a privacy by design approach and to use Privacy Impact Assessments (or Data Protection Impact Assessments as they will be known) in certain circumstances.

11. Data Protection Officers

It will be a statutory requirement to designate someone to take responsibility for data protection compliance, known as the Data Protection Officer (DPO).

The DPO must have access to information across the Council and have the support of the leadership to carry out their role. The Council has approached three neighbouring Councils for quotes for the provision of a shared DPO. Two were not interested and only South Staffordshire Council has quoted and has been assisting in the preparation of compliance towards GDPR. It is proposed that the Assistant Director Democratic & Regulatory Services from South Staffordshire Council is designated as a shared DPO for Lichfield District Council and will be invited to attend Leadership Team meetings/Legal & Democratic team meetings as and when required. The Council will receive a designated Solicitor for 1 day per week who is trained in GDPR. The team at South Staffordshire Council which consists of 4 solicitors will also provide advice and assistance on day to day GDPR issues and on Information Governance as and when required.

12. International

There are provisions for those organisations operating in more than one EU state but these are not applicable to the Council.

In order to ensure the Council is GDPR compliant, the following actions are also being taken:

a) A Service Level Agreement is currently being drafted;

b) **Review any contracts it has with 'data processors' i.e. external organisations who process personal data on behalf of the Council.** GDPR requires the Council as a controller of data to ensure that any processor complies with new legal requirements;

b) Review the existing 'organisational' and 'technical' measures it has in place and ensure that personal data is kept 'safe';

c) Review and update its incident management plan and formulate procedures setting out when and how to notify the Commissioner and affected individuals if there was a breach of security i.e. unauthorised or unlawful processing, loss, damage or destruction of personal data.

3.3 Next Steps

Whilst preparation work has been underway for some time, there is still a significant amount of work to be undertaken over the coming months.

Meetings are now being arranged with representatives of service teams to provide the necessary training/information in the drafting and giving of 'fair processing notices' to all individuals from whom the Council collects information from.

The meetings will also identify any data processor contracts that need to be looked at.

It is anticipated that these meetings will have all taken place by the end of April 2018. It will then be for service teams to draft the appropriate notices (with guidance and support) and to liaise with any current processors of data that the Council controls. Revised contract provisions, to take account of the new GDPR requirements are being finalised and will be made available to all service teams and incorporated into the Council's Standard Terms and Conditions.

Procedures to assist when people exercise rights have been drafted and the revised data protection policy is being finalised and will come forwards for approval shortly.

Discussions will take place with ICT re: any technical changes that may need to take place to keep data safe. These discussions will also inform the revision of the Council's current incident management plan. It is planned to complete the revision of the Council's information security policy/incident management plan by the end of April 2018.

A number of staff have already received training on the changes brought about by GDPR via team training sessions provided in-house. All those staff who regularly handle personal data will have received face-to-face training before the coming into force of the GPDR and those who do not will have undertaken an appropriate form of e-learning. The training programme will be risk-based with those service teams that handle the most/most sensitive data being targeted first; these areas will receive face-to-face training. It is envisaged this will include Revenues and Benefits, Human Resources, Elections, Development Management and Local Plans. Records will be kept of all training undertaken.

Conclusion

The Council is on track to meet the requirements of the new data protection rules. There will be a substantial amount of work between now and 25 May 2018, however, we are confident that we will be compliant with the new rules on the go-live date.

Regular updates will be given to Members on preparation for the changes to the data protection rules.

Alternative Options	The Council could have appointed an In-house DPO, but the costs including overheads would have been much greater. Having a shared service with South Staffordshire Council brings resilience as they have a team of experts on data protection issues/information governance as well as providing the services of a DPO.
Consultation	Report to Audit Committee – 27 March 2017
Financial Implications	The sum of £20,000 per year on GDPR has been included within the approved MTFS and is within budget.
Contribution to the Delivery of the Strategic Plan	Proposals will assist with compliance with the legal requirements and thus the Council's ability to deliver the services required and Fit for Future.

Equality, Diversity and Human Rights Implications	The new General Data Protection Regulations contain 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. However, analysis of the equality implications have been included as part of the wider project plan when considering the impact the regulations will have on each service. These will be included in future reports if necessary.
Crime & Safety Issues	No crime and safety issues.

	Risk Description	How We Manage It	Severity of Risk (RYG)
A	Non Compliance with Legislation.	The Data Protection Policy is based on the current best practice. GDPR Training will need to be provided to all employees and members. The updated Data Protection Policy will be published on the Council's Intranet and Website once agreed. It will also be informed to all employees of the Council.	State if risk is Red (severe), Yellow (material) or Green (tolerable) as determined by the Likelihood and Impact Assessment. YELLOW
B			
C			
D			
E			

Background documents: Regulations (EU) 2016/679 of the European Parliament and of Council of 27 April 2016 and the Protection of Natural Persons with regard the processing of personal data and on the free movement of such data and repealing the direction 95/46/EC (General Data Protection Regulations).

Relevant web links: https://democracy.lichfielddc.gov.uk/mgListCommittees.aspx?bcr=1