BOROUGH COUNCIL OF WELLINGBOROUGH **AGENDA ITEM** **6**

Partnerships and Performance Committee **18 June 2018**

Report of the Assistant Director

General Data Protection (GDPR) progress report

1 Purpose of report

This report has been prepared to present members with an overview of how the council is meeting its obligations with the General Data Protection Regulation (GDPR), which was implemented on 25 May 2018.

2 Executive summary

Over the last 18 months the council has been obligated to review its data protection application and update, where relevant, it's handling of personal and special category data and ensure that the fundamental rights and freedoms of individuals are upheld and safeguarded.

3 Appendices

Appendix 1: Extract from the internal audit progress report 2017/18.

4 Proposed action:

Members are invited to resolve to note the progress made in relation to the GDPR implementation.

5 Background

5.1 In August 2016 a report was presented to senior management team (SMT) to inform them of the impending EU regulation 2016/679 due to come into force on 25 May 2018, which would repeal the Data Protection Act 1998 and implement the General Data Protection Regulation.

5.2 It was recommended that the council undertook the following actions by 25 May 2018 to ensure compliance with the GDPR:

- An information audit of all paper and electronic records (including all corporate systems) be undertaken to identify what personal data is held, how long it is held for, what it is used for and who it is shared with.
- Adoption of a detailed document retention schedule specific to the information we collect.
- The above information to form an information asset register that must be accurate and kept up-to-date

- All privacy/fair-processing notices to be reviewed and re-written with consideration given to how consent to collect information is obtained.
- Internal processes established and documented to ensure the council can demonstrate compliance e.g. breach reporting, right of access requests, privacy impact assessments (PIA's), consent opt-outs etc.
- Data protection training for all employees on induction and then at least every 2 years thereafter.
- A project board should be established and a project plan developed.
- Risks should be identified and added to risk register.
- Responsibilities for tasks should be allocated.
- Develop a communication plan and training schedule.

5.3 Following the report to SMT a project sponsor, a project manager and project support were appointed for the GDPR project, involving members of the senior management team to acknowledge the importance of good data management.

5.4 In approaching GDPR, it was considered beneficial to approach other local authorities, such as East Northants Council due to having a shared ICT/Information Governance Manager and Kettering Borough Council and Daventry District Council because of the District Law partnership.

5.5 It was also agreed that the Senior Organisational Development Officer would continue to work closely with officers in the countywide Northamptonshire Access to Information Group (NAIG) to share best practice and develop common processes where practical.

6 Discussion

6.1 In February 2018 the council's external auditors, CW Audit, finalised their Internal Audit Report 2017/18 on the council's GDPR preparedness (Appendix 1). The audit concentrated on providing an independent assessment of progress made to implement GDPR and detail the arrangements in place to complete the necessary work by the May 2018 implementation deadline. The audit concluded that the BCW had made appropriate arrangements to implement GDPR.

6.2 All relevant policies have been uploaded to the council's intranet system and the website, including the privacy policy, breach policy and subject access request procedure. Information asset registers have been uploaded to the website for transparency; this is in a bid to reduce in freedom of information requests.

6.3 Members were provided with a briefing session on GDPR to highlight their obligations in this regard within their roles in the community and the requirement for them to register as data controllers with the Information Commissioners Office (ICO).

6.4 With regard to staff awareness, an e-learning module has been provided for all employees to complete and this will be followed up with classroom training

for key officers.

6.5 Further Actions:

- To upload service area information asset registers and breach reporting log to Resilience direct.
- To undertake a yearly internal review of data protection compliance to streamline the handling of data and promote best practice across the council.
- To provide assurance to members via an internal GDPR Audit.
- Present the internal GDPR audit report to the Partnerships and Performance Committee at the end of May/beginning of June of each subsequent year.

7 Legal powers

The council has a statutory duty to comply with the changes made by the EU regulation 2016/679 and the UK Data Protection Bill.

8 Financial and value for money implications

None identified.

9 Risk analysis

Nature of risk	Consequences if realised	Likelihood of occurrence	Control measures
Non-compliance with EU Regulations, leading to potential legal challenge, financial risk and reputational damage.	A maximum fine of €20m or 4% of annual turnover.	Low	Implement the necessary legislative changes and reflect in BCW's policies and procedures. Ensure staff and members are aware of the changes and trained by the 25 May 2018.

10 Implications for resources

The work required to guide the council to compliance with the GDPR has been resource intensive across the authority. The council is also required to appoint a Data Protection Officer who is independent of data handling on a day to day basis. This is currently the Governance Officer.

11 Implications for stronger and safer communities

The council takes its obligations seriously to protect the personal data it holds and handle it in line with GDPR. By its own nature, the council holds highly sensitive information in certain services, such as benefits and housing, and data handling is of the utmost importance across the organisation.

12 Implications for equalities

None identified.

13 Author and contact officer

Naomi Harewood Governance Officer

14 Consultees

Karen Denton, Principal Corporate Support Manager

15 Background papers

- 2016 GDPR Report to SMT.
- Appendix 1: CW Audit's Internal Audit Report 2017/18 on BCW's GDPR Preparedness (extract).

Borough Council of Wellingborough

Internal Audit Report 2017/18
18BCW_15 – GDPR Preparedness
FINAL

February 2018

cw audit

internal audit services

1. What we found in summary

As this piece of work was undertaken as an exercise to establish the Council's state of preparedness for implementing the GDPR by May 2018, an overall audit opinion that contributes towards our year end opinion is not appropriate and has not therefore been provided. The audit concentrated on providing an independent assessment of progress made thus far to implement GDPR and arrangements in place to complete the necessary work by the May 2018 implementation deadline. The audit concluded that the Council has made appropriate arrangements to implement GDPR. Key actions taken thus far include:

- Identification of dedicated resource to drive forward the key workstreams necessary to implement GDPR (Governance Officer, supported by the Electoral Services Team Leader).
- Development of a detailed action plan that identifies key workstreams and targets for completion.
- Regular progress reports on implementation of GDPR to the Senior Management Team (SMT).
- Compilation of draft Information Asset Registers is almost complete, with work now commencing on production of data flow maps.

The action plan identifies a challenging work programme over the next few months. Key actions still to be completed include:

- Gap analysis of data flow maps once complete to identify further work necessary in relation to include consent (where applicable), lawful basis for processing data, storage, sharing agreements and usage (relative to consent), retention, archiving and disposal.
- Review privacy notices/statements and develop Council wide privacy notice.
- Comprehensive review/compilation of a number of policies related to various aspects of GDPR.
- Develop Privacy Impact Assessment forms and produce guidance for staff.

The audit has confirmed that the action plan contains the key workstreams necessary to implement GDPR by May 2018, but given the amount of work left to deliver, it is not possible to at this stage to confirm that the action plan will be fully achieved by that date. The auditor is however of the opinion that sufficient work will have been completed by May 2018 to demonstrate to the Information Commissioner's Officer (ICO), should the need arise, that the Council has responded appropriately to the requirements of GDPR.

Whilst the audit was able to confirm the existence and ongoing delivery of a robust action plan, the review highlighted some further areas that the Council may wish to consider when delivering the GDPR agenda. With this in mind, a number of recommendations have been made in section 4 of this report.

2. The context for our review

General background

The Information Commissioner has provided guidance on preparing for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018. This includes the following commentary:

"Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is essential to start planning your approach to GDPR compliance as early as you can and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Note that some parts of the GDPR will have more of an impact on some organisations than on others (for example the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process."

3. What we agreed to do

The overall objective of the review was to assess the extent to which the Council is making progress towards implementing GDPR by the May 2018 deadline. The key risks associated with failure to implement GDPR are detailed below, as well as the key GDPR areas that need to be addressed.

The key risks	• Non compliance with EU Regulations, leading to potential legal challenge, financial risk and reputational damage.
GDPR areas	• Awareness • Information you hold • Communicating privacy information • Individual's rights • Subject access requests • Legal basis for processing personal data • Consent • Children • Data Breaches • Data Protection by Design and Data Protection Impact Assessments • Data Protection Officers • International

We have delivered this review in accordance with the statements made in Appendix 2.