Audit Committee

29th March 2018

Report of: **Shahzia Daya, Service Director Legal and Democratic Services and SIRO**

Title: **Update on the General Data Protection Regulation (GDPR) readiness**

Ward: City Wide

Officer Presenting Report: Quentin Baker, Interim Director Legal and Democratic Services

Recommendation

To note steps taken to implement the General Data Protection Regulations

Summary

The Council's has completed preparations for the new data protection rules that came into effect on 25 May 2018 and the current project is being formally closed. An outline business case has been developed with options for how this can be further developed and embedded into the organisation so that good data protection practices can be maintained going forward.

The significant issues in the report are:

No significant issues

Policy

1. Compliance with legislation is a statutory requirement. Good data protection also maintains public confidence and supports partnership working.

Consultation

2. Internal
Deputy Mayor and Cabinet member for Finance, Governance & Performance

3. External
Not applicable to this report

Context

4. The General Data Protection Regulation (GDPR) came into effect across the EU on 25 May.

5. A project board was established in Nov 2017 worked hard (meeting weekly from February 2018) to deliver the essential elements of compliance required by that date. That project deliverables have has now been completed and it is in the process of being formally closed. What has been delivered is:

- Colleagues who routinely access ICT systems have been trained in the new data protection rules according to their job role those who do not routinely access ICT systems have received a briefing;
- An audit of all personal data held by the council has been completed and documented in a record of processing activity, or ROPA, for each service;
- Privacy notices have been published on the Council's web site for each service, informing service users how their data will be used and their rights. Over 150 new notices have been published on the council's web site;
- Agreements with partners have been reviewed where personal data is shared;
- Consents have been reviewed and refreshed where necessary to GDPR standards where this is relied on a legal basis for processing;
- New centralised processes are in place for handling Subject Access Requests and Data Breaches;
- A new requirement has been introduced to carry out a Privacy Impact Assessment as part of the change business case and decision making process;
- The data retention schedule has been refreshed and processes put in place to implement this;
- 1,200 supplier contracts have been updated to include GDPR specific clauses, targeting the highest risk contracts as a priority;
- The role of statutory data protection officer, which is a mandatory requirement for Public Authorities under the regulation, has been assigned to the Monitoring Officer;
- The data protection policy has been updated to reflect GDPR requirements;
- Support has been provided to the Bristol companies, Councillors and Schools.

6. Under GDPR organisations are required to ensure that they are able to demonstrate their compliance on an ongoing basis. While the Council has put in place the key building blocks for

the 25 May, further work is needed to embed GDPR into the organisation so that compliance can be maintained in the years ahead. In practice that means:

- Having a plan in place for training people joining the organisation and refreshing knowledge of a periodic basis, according to their job role
- Clarifying job roles and responsibilities for maintaining compliance and key documentation
- Updating the remaining supplier contracts
- Ensuring ICT systems meet GDPR requirements
- Processes for handling other types of request such as the right to be forgotten

Other Options Considered

7. There are options for concluding this work and an outline business case (OBC) has been developed to seek agreement on the way forward.

8. The option recommended by the project board and endorsed by the Statutory Data Protection Officer is to set up a 'phase 2' project that will complete the activities listed above and build the necessary structures in order to hand the project over to business as usual in a controlled manner.

Risk Assessment

9. GDPR was identified as a high-rated risk. The actions taken have now significantly reduced the current level of risk. The likelihood of issues arising has been greatly reduced, although the potential impact remains the same. GDPR is now a 'medium' rated risk.

10. Maintaining compliance is key to continuing to mitigate this risk in the years ahead. The outline business case assesses the organisations data protection risk tolerance and evaluates each option to identify the extent to which the ongoing risk will be mitigated.

Public Sector Equality Duties

11. The project board considers the requirements of the Equalities Act duties when considering implementation of the GDPR legislation and embedding best practice

Legal and Resource Implications

Legal

Legal advice provided by Shahzia Daya, Service Director of Legal and Democratic Services

Financial
(a) Revenue

(b) Capital
Financial advice provided by Kevin Lock, Finance Manager

Land/Property

Not applicable

Human Resources

HR advice provided by Mark Williams, Head of Human Resources 14 March 2017

LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985
Background Papers:
None