

# Audit Committee

29th March 2018



**Report of:** Shahzia Daya, Service Director Legal and Democratic Services and SIRO since 15<sup>th</sup> February 2018

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

**Ward:** All

**Officer Presenting Report:** Shahzia Daya

## Recommendation

To note progress being made with regard to the Council's compliance with the General Data Protection Regulations

## Summary

The report outlines progress of the Council's preparations for the new data protection rules that come into effect on 25<sup>th</sup> May 2018.

## The significant issues in the report are:

The project as originally defined had an ambitious plan to achieve full compliance by the 25<sup>th</sup> May. Due to capacity, a risk based approach is now being taken which will see the key building blocks in place by the 25<sup>th</sup> May. The project has moved into 'exception' status and an action plan is being worked on to bring the project back on track to enable the Council to be GDPR compliant by 25<sup>th</sup> May. Key to this will be stronger project governance, resource allocation across the authority and an assessment of risk to identify key priorities to improve compliance on an on-going basis.



## Policy

1. Compliance with legislation is a statutory requirement

## Consultation

2. **Internal**  
Deputy Mayor and Cabinet member for Finance, Governance & Performance
3. **External**  
Not applicable to this report

## Context

4. This report outlines the Council's plans, current progress and risks regarding preparations for the new Data Protection rules under the EU's General Data Protection Regulation (GDPR).
5. GDPR becomes directly applicable across the EU on the 25th May 2018. These new rules are the biggest change to data protection for twenty years and are designed to harmonise across the EU and to bring them up to date in the 'Information Age'. GDPR applies to any organisation trading with the EU and as a result GDPR will be enacted into UK law; a draft Data Protection Bill is currently passing through Parliament.
6. The UK's Information Commissioners Office (ICO) has set out twelve steps that organisations should be taking to prepare for compliance and this is the basis of the Council's comprehensive project plan. The ICO advise that compliance is an ongoing effort in which organisations have to show they have put the key building blocks in place:
  - Understanding the information already held;
  - Implementing accountability measures;
  - Ensuring appropriate security; and
  - Providing appropriate training for staff.
7. Progress has been made towards putting these in place. Actions taken to date:
  - Updated data protection and GDPR training has been launched across the Council. This is mandatory for all staff and the end of March has been set as the deadline for everyone to complete the training which sets out the basic principles of GDPR;
  - The audit of personal data has progressed with eighty-four percent drafts and fifty-four percent final completed thus far. There are over one hundred audits being completed and some contain details of over three hundred different data sets. This audit will be completed before 25<sup>th</sup> May 2018;
  - Privacy Impact Assessments (PIA) have been introduced and integrated into the business case process for **new** change initiatives. This has resulted in five completed with a further eleven currently in progress. There will be about eighty to complete for existing ICT systems which hold very sensitive personal data;
  - New contracts involving processing of personal data are being made GDPR compliant and over one thousand existing suppliers have been contacted to initiate the necessary changes

to existing contracts and gain assurances over suppliers' ability to meet the new rules. There are over two thousand one hundred existing contracts to be updated;

- New and updated privacy notices are being drafted and so far thirty percent of services have completed these. There will be approximately five hundred new privacy notices needed;
- The way we handle subject access requests is under review with an assessment of the 'as-is' nearing completion. This work will then focus on the key changes required under the new rules. This will be concluded in April;
- A Data Protection Lawyer has been appointed to provide independent advice to schools under the trading with schools programme;
- The visibility of the project has significantly increased with weekly reporting to the Deputy Mayor, Executive Directors and Service Directors as a standing agenda item at their meetings. The project board itself is now meeting weekly.

8. In terms of direction of travel, there remains a significant amount of work to be done. What we are doing next is:

- Completing key documentation and record keeping requirements supported by action plans which will be produced by tier three managers. This work includes the data audit, Privacy Impact Assessments, data sharing protocols, data retention and deletion, and reviewing and refreshing consents;
- Holding focussed workshops to train data custodians across the organisation on these specific areas of competence;
- Completing the data protection training across the Council. This requirement will include Members, who access Council systems to carry out their roles;
- Progressing contractual changes for existing suppliers, prioritising this on a risk managed basis (i.e. contracts processing the highest volumes of the most sensitive-personal data the council holds being targeted first);
- Seeking assurance from council owned companies and understanding what support may be required;
- Progressing definition, evaluation and recruitment of a statutory data protection officer and their team to carry out the required functions created by GDPR;
- Introducing a centralised process for handling the expanded range of subject access rights.

9. The project as initially defined had an ambitious plan to achieve full compliance by the 25th May. Due to capacity a risk based approach is now being taken which will see the key building blocks in place by the 25<sup>th</sup> May, including:

- Training completed council-wide
- Processes for handling subject access requests
- Record of processing activity
- New contracts will be GDPR compliant
- Updated privacy notices
- Privacy Impact Assessment (PIA's) completed
- Consent forms updated
- Old data reviewed and deleted

10. The project has moved into 'exception' and an action plan has been developed to bring the project back on track to enable the Council to be GDPR compliant by 25<sup>th</sup> May. This will address the key findings of the internal audit report. Key to this will be stronger governance, resource allocation across the authority and an assessment of risk to identify key priorities to improve compliance on an ongoing basis.

### Other Options Considered

11. Not applicable to this report

### Risk Assessment

12. Project risks are managed by the project board and a log of risks is maintained

### Public Sector Equality Duties

13. The project Board takes account of the Equalities Act duties when considering implementation of the GDPR legislation

### Legal and Resource Implications

#### Legal

The date for GDPR compliance is 25 May 2018. Any gaps in the Council's compliance highlighted in this report and as a result of the ongoing project will need to be addressed.

**Legal advice provided by** Shahzia Daya, Director – Legal & Democratic Services

#### Financial

##### (a) Revenue

We set up a reserve of £91k for expenditure planned for this year but as we are able to contain this year's expenditure in revenue we do not need to draw down from it. We are also planning to boost the reserve up at year-end depending on outturn.

##### (b) Capital

GDPR has received the requested £91k funding from reserves and further expenditure will be authorised through the ongoing revenue budget and GDPR reserve. The appropriate levels of funding will be reviewed in-line with the business case.

**Financial advice provided by** Kevin Lock, Finance Manager

#### Land/Property

Not applicable

#### Human Resources

Staffing requirements will be agreed in the business case and any appointments to new roles will be made in accordance with the Council's Recruitment and Selection Policy.

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

### LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985

#### Background Papers:

None