Committee(s)	Dated:
Information Technology Sub-committee	22/03/2018
Subject: General Data Protection Regulation (GDPR) update report	**Public**
Report of: Michael Cogher, Comptroller & City Solicitor	**For Information**
Report author: Michael Cogher, Comptroller & City Solicitor,	

Summary

This report summarises the new requirements of the General Data Protection Regulation (GDPR) and progress of the GDPR project toward securing compliance with it by 25th May 2018. GDPR substantially updates data protection law, including changing conditions for processing, strengthening privacy and other rights and increasing penalties for breaches of the rules.

Recommendations

Members are asked to note the report.

Introduction

1. The current data protection regime is based on an EU Directive from 1995 and implemented in the UK by the Data Protection Act 1998. Since then there have obviously been significant advances in IT and fundamental changes to the ways in which organizations and individuals communicate and share information.

2. As a result the EU has introduced updated and harmonized data protection regulations known as the General Data Protection Regulation ("GDPR") which is due to come into force on 25 May 2018.

3. It will be implemented in the UK, notwithstanding Brexit, by legislation announced in the Queen's Speech.

4. This Report outlines the steps that the Corporation is taking to ensure that it is GDPR compliant.

Impact

5. The Information Commissioner's Office (ICO) which is responsible for guidance and enforcement of data protection has said:

"Many of the principles in the new legislation are much the same as those in the current Data Protection Act. If you are complying properly with the current law, then you have a strong starting point to build from. But there are some important new elements, and some things will need to be done differently".

6. GDPR introduces several new concepts and approaches. Equally many of the existing core concepts of personal data, data controllers and data processors are broadly similar. It remains founded on a principle based approach.

7. Whilst much detail and particularly the domestic legislation and ICO guidance is not yet available the Corporation needs to review its organisational and technical processes both corporately and departmentally.

GDPR Project Progress

8. Preparations for GDPR are well underway and in summary involve a review of the Corporation's information governance practices, policies and procedures; training and awareness raising; and ensuring the necessary technical IT and information security systems are GDPR compliant.

   These tasks are the subject of a detailed project plan overseen by the Information Board and IS Steering Group and delivered by the GDPR Project Team and departmental Access to Information Network Representatives (AIN) and management teams.

9. The Comptroller & City Solicitor was formally appointed by committee as the Corporation's Data Protection Officer in November 2017.

10. The GDPR implementation project plan covering all tasks required to effectively prepare for GDPR compliance was created in September 2017 and audited by Mazars with a positive outcome and with no minor or major risks to project delivery identified.

11. Information governance

    - GDPR Corporate Risk CR 25 was created and agreed by Audit & Risk Committee.
    - GDPR compliance requirements and project plan reported to Policy & Resources, Establishment Committees and IT sub-committee.
    - Project delivery is controlled by three weekly Project Team stage control meetings which monitor progress, capture GDPR issues and risks, assess required changes and associated corrective action and allocate work packages. The Project Team reports to the Information Board and IS Steering Group, additionally update reports and revised policies are reported to Policy & Resources and Establishment Committees and to IT sub-committee.
    - Regular liaison with IT workstreams are taking place which are reported to the GDPR Project Team for action and to the Information Board.

12. Training and Communication

    - Six half day training sessions to AIN representatives and key staff delivered by the Comptroller & City Solicitor and Senior Information Compliance Officer all AIN representatives have undertaken the initial training

- Two training sessions for Members have been delivered with two more planned
- GDPR detailed guidance notes issues to AIN representatives.
- Monthly 'drop in' training sessions scheduled until April 2018
- Further training sessions are planned on GDPR specifics such as privacy impact assessments, ROPA, fair processing notices, breach notifications etc
- Chief Officer updates are provided at COG, senior managers nominated as leads in each department, senior manager training sessions scheduled
- Mandatory e-learning course is in the final stages of development in liaison with HR
- GDPR corporate communications plan agreed with Communications Team with an initial roll out in March 2018 with a follow up in May 2018, will include
- A dedicated GDPR intranet page is in development to include guidance, news, policies, procedures, the relevant forms and FAQ's
- Detailed guidance tailored to departments has been delivered and will continue as department specific GDPR issues and risks arise
- Corporate GDPR communications plan agreed and scheduled with major awareness campaigns in April and May 2018
- Dedicated GDPR intranet page created with GDPR guidance, Q&A's, news and the project plan

13. Policies:

- GDPR related policies are currently being revised to incorporate GDPR requirements these are Employee Data Protection Policy, Data Protection Policy, Subject Access Rights Policy, Pupil and Parent Data Protection Policy, Data Breach Policy, Information Security Policy, Storage of Data Policy, Email use policy, System Vulnerability Policy, Encryption Policy, Security Patching Policy.

14. Procedures:

- GDPR requires a record of processing activities (ROPA), a proforma was issued to departmental AIN representatives, the returns are being analysed by the Information Compliance Team who will develop and maintain the central record which will include the reasons for collection and retention
- Subject Access Request procedures are currently being revised
- C&CS Contracts Team are liaising with contractors as data processors on GDPR requirements compliance
- Privacy Impact Assessment template is currently being tested on the CRM project
- Communicating Privacy Information requirements included in the ROPA returns from which the procedure will be developed
- Privacy Notices currently being drafted

- Data Breach procedures and template form drafted

15. Information Technology Systems:

- Audit of IT contracts to ensure new responsibilities is underway
- Two potential providers of a software solution to identify and resolve high risk to storage and processing of personal data and identify where a retention schedule is required are providing proof of concept
- Exchanging GDPR good practice with two local authorities
- IT systems capability to support Privacy Impact Assessments are being developed
- Information retention schedules and the right to be forgotten are being developed
- Applications Development and Support will start to test major applications that process personal data against the right to erasure
- On line internal Data Breach Notification form is being developed
- Drive rationalisation and security guidelines to be implemented

Validation of Approach & Implementation

16. Because of the risks presented by GDPR it has been agreed that a second review of the Corporation's approach and delivery of policies and procedures to meet the requirements will be undertaken by its internal auditors, Mazars, in mid-April 2018 and their findings reported to Summit and committees as appropriate.

Conclusion

17. GDPR places significant obligations on the Corporation in relation to the processing of personal data to protect the rights and freedoms of everyone.

    The GDPR project has made significant progress, is anticipated that the Corporation will be generally compliant with GDPR requirements by May 25 2018.

Appendices

None

Michael Cogher
Comptroller & City Solicitor
0207 332 3699
michael.cogher@cityoflondon.gov.uk