Committee(s)	Dated:
Information Technology Sub-committee	31/05/2018
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) which came into force on 25th May 2018 and progress of the GDPR project toward securing compliance with it. 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 organisations and individuals communicate and share information.

2. As a result, the EU has introduced updated and harmonised data protection regulations known as the General Data Protection Regulation ("GDPR") which came 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. The Corporation is reviewing organisational and technical processes both corporately and departmentally. The basic governance and technical systems required for GDPR compliance will be in place by 25th May. However, these will need to be bedded in, refined and reviewed on an on-going basis as GDPR becomes "business as usual".

GDPR Project Progress

8. The first phase of the Corporation's preparations for GDPR are at the time of writing close to completion and in summary have involved 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. A further audit was undertaken by Mazars in May 2018 to assess the Corporations readiness and levels of compliance with GDPR requirements the outcome of which will be fed into phase two of the GDPR project.

11. A phase two GDPR project running from 25 May 2018 to 31 December 2018 has been created and resourced the aim being to further embed and refine GDPR knowledge and compliance across the Corporation.

12. 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 at bi-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.

13. Training and Communication

- Six half day training sessions for AIN representatives and key staff delivered by the Comptroller & City Solicitor and Senior Information Compliance Officer all AIN representatives have undertaken the initial training. Further focused training has been provided to the HR Department, Remembrancer's Events Team and EDO.
- Five training sessions for Members have been delivered, and member guidance substantially revised to incorporate GDPR requirements, template forms issued including RoPA, Privacy notices
- GDPR detailed guidance notes issues to AIN representatives.
- Further training sessions are planned on GDPR specifics such as privacy impact assessments, ROPA, fair processing notices, breach notifications etc. post May 25th to refine and embed policies and procedures
- Chief Officer updates are provided at COG, senior managers nominated as leads in each department, senior manager training sessions scheduled
- A mandatory GDPR e-leaning training package was launched on City Learning on 23 April 2018 compliance levels are being monitored by the Data Protection Officer and reported to Chief Officers, the deadline for staff to undertake the training is 24 May 2018, also available to members
- GDPR corporate communications plan was agreed with the Communications Team and launched on 8 May 2018
- A dedicated GDPR intranet page has been updated 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

14. Policies:

- GDPR related policies have been revised to incorporate GDPR requirements including Employee Data Protection Policy, Data Protection Policy, Subject Access Rights Policy, Pupil and Parent Data Protection Policy, Data Breach Policy, Appropriate use of IT Policy, Storage of Data Policy, Email use policy, System Vulnerability Scanning Policy, Security Patching Policy and Procedure.
-

15. Procedures:

- GDPR requires a record of processing activities (ROPA), a proforma was issued to departmental AIN representatives, the returns have been

analysed by the Information Compliance Team who and included in a central record which will include the reasons for collection and retention.

- Subject Access Request procedures have been revised
- Standard contract clauses and data processing agreements have been updated and circulated to departments for issue to all existing contractors and existing agreements
- 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 have been revised and agreed, layered privacy notices are now on the CoL website incorporating all required generic elements under which sit layers of function specific information
- Data Breach procedures and template form revised
- Legal basis for employee personal data has been reviewed and revised
- Lawful basis for processing personal data procedures reviewed and revised
- Privacy Impact Assessment (PIA) procedure revised

16. Information Technology Systems:

- Major service providers have been sent Data Protection Schedules to ensure they agree to new responsibilities
- Agile Solutions and Agilisys to provide proof of concepts during May for a software solution to identify and resolve high risk to storage and processing of personal data and identify where a retention schedule is required
- IT systems capability to support Privacy Impact Assessments (PIA) are being developed; PIA form to be finalised and created as an on-line document
- 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

17. Because of the risks presented by GDPR a second review of the Corporation's approach and delivery of policies and procedures to meet the requirements was undertaken by its internal auditors, Mazars, in May 2018, their findings will be reported to Summit and committees as appropriate.

Conclusion

18. 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, subject to the findings of the Mazars audit it is anticipated that the Corporation has achieved baseline compliance with GDPR requirements, further work will be required to embed, reinforce and enforce compliance with GDPR requirements across departments.

Appendices

None

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