Committee	Date
Establishment Committee	17/10/2017
Subject: General Data Protection Regulation Report	**Public**
Report of: Michael Cogher Comptroller & City Solicitor	**For Decision**

Summary

This report sets out the new requirements of the General Data Protection Regulation (GDPR) and the work required by the Corporation to secure compliance with it by 25th May 2018.

Recommendations

That Summit Group

1. Note the report.

2. Endorse the general approach.

3. Endorse the proposal that the Comptroller & City Solicitor be appointed as the Corporation's Data Protection Officer and that a report be taken to the relevant Committees in the September cycle making this recommendation.

1. Introduction

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.

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.

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

This Report outlines the steps that the Corporation will need to take in order to ensure that it is GDPR compliant.

2. Impact

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".

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 principles based approach.

Whilst much detail and in particular the domestic legislation and ICO guidance is not yet available the Corporation needs to review its organizational and technical processes both Corporately and Departmentally.

3. Key Changes

The principal changes relevant to the Corporation are briefly summarized below:-

1. **Increased enforcement powers** – fines for breaches of the DPA are currently limited to £500,000. This will be increased to £10 million or 2% of annual turnover or £20 million or 4% of annual turnover depending on the nature of the breach, with the latter applying to breaches of the data protection principles and data subject rights.

2. **Consent will be harder to obtain** – consent is one of the various conditions which can be relied on for processing and the GDPR will require a higher standard of consent by clear affirmative action demonstrating a freely given, specific informed and unambiguous consent. The burden of proof for establishing this will be on the data controller. It will therefore be necessary to review current processing based on consent to ensure that it will meet the new standards or identify alternative grounds for processing. In addition, Public bodies will no longer be able to rely on their own "legitimate interests" for processing and will again have to identify alternative grounds – this is likely to be that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority in most cases. (NB it is anticipated that the Corporation's hybrid nature will be properly reflected in the legislation).

3. **A risk based approach to compliance** – organizations will bear responsibility for assessing the degree of risk that their processing activities pose to data subjects. This is reflected in the "privacy by design and default" provisions and other requirements described below.

4. **Privacy by design and default** – having regard to the state of the art and the cost of implementation and the nature, scope and context of the processing, organizations will be required to implement data protection "by design and by

default" at the time of determination of the means of processing and the processing itself. This recasts and strengthens the current duty under the Seventh Data Protection Principle.

5. **Privacy Impact Assessments (PIA'S)** – organizations will be required to carry out PIAs before introducing processing by new technologies likely to pose a risk to data privacy and in other circumstances to be specified. Mandatory consultation with the ICO may be required in certain circumstances.

6. **Records of Processing Activities** – organizations will need to maintain detailed documentation recording their processing activities. The information required includes the purposes of the processing, categories of data subjects, personal data, and those to whom data will be disclosed and general technical and security measures in place.

7. **Appoint a Data Protection Officer** – certain organizations, including all public authorities, will have to appoint a Data Protection Officer. This is dealt with in more detail below.

8. **New Breach Notification Rules** – breaches will have to be notified to the ICO within 72 hours where feasible unless the breach is unlikely to result in risk to individuals. Where a high risk to individuals arises they will also have to be notified unless an exception applies.

9. **Additional Rights for Individuals** – these comprise the right to be forgotten, a right to object to profiling and to data portability.

10. **Less Time for Subject Access Requests** – the time limit for responding to SAR's will be reduced from 40 days to 1 month and the information which must be provided will be extended.

4. Appointment of a Data Protection Officer (DPO)

As a public authority the Corporation will be required to appoint a DPO whose minimum tasks are defined in Article 39 as:

- To inform and advise the organization and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

It is recommended that the DPO holds a senior position in the organisation with direct access to "board" level. In the Corporation's context it is therefore recommended that the Comptroller and City Solicitor who currently manages the Data Protection and Freedom of Information Compliance Team and acts as SIRO and chairman of the Information Board be appointed as DPO and that the necessary report be presented to relevant Committees in the September cycle.

5. Preparation and Project Plan

Preparations for GDPR will 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 will be the subject of detailed project plans to be overseen by the Information Board and IS Steering Group.

(a) Information Governance

Work in this area will include:-

- A programme of awareness raising and training from September 2017
- Documenting data held (including considering the reasons for its collection and retention)
- Reviewing Privacy Information
- Inclusion of new rights into policies
- Amending Subject Access Request procedures
- Reviewing the basis of processing (particularly in relation to consent and future lack of reliance on "legitimate interest" grounds qua public body)
- Reviewing the Data Breach procedures
- Ensuring procedures incorporate data protection by design and default
- Reviewing relevant contractual provisions

(b) Information Technology Systems

Work in this area will include:-

- Audit of IT contracts to ensure new responsibilities of IT Suppliers are adequately provisioned for
- Review of systems capability to support Privacy Impact Assessments – Privacy requirements to be specified in any new IT contracts
- Information retention schedules and the right to be forgotten
- Review and changes to IT policies impacted by GDPR responsibilities

6. Validation of Approach & Implementation

Because of the risks presented by GDPR it has been agreed that a review of the Corporation's approach will be undertaking by its internal auditors, Mazars, and their findings reported to Summit and committees as appropriate.

It is proposed that the Governance and IS Project Plans will be reviewed in August 2017 and with an audit of progress against the Plans taking place in January 2018.