

**Manchester City Council  
Report for Information**

**Report to:** Resources and Governance Scrutiny Committee – 19 July 2018

**Subject:** Update on implementation of the General Data Protection Regulation (GDPR)

**Report of:** City Solicitor

---

**Summary**

To set out the impact of GDPR on the Council and update the Committee on the work done to implement GDPR including mitigating the loss of personal data.

**Recommendations**

The Committee is asked to note this report

---

**Wards Affected:** All

---

**Alignment to the Our Manchester Strategy Outcomes (if applicable)**

<b>Manchester Strategy outcomes</b>	<b>Summary of how this report aligns to the OMS</b>
A thriving and sustainable city: supporting a diverse and distinctive economy that creates jobs and opportunities	Not directly applicable
A highly skilled city: world class and home grown talent sustaining the city's economic success	Not directly applicable
A progressive and equitable city: making a positive contribution by unlocking the potential of our communities	Implementation of the GDPR will lead to enhanced rights for individuals and strengthen trust that personal information is being handled well as well as increasing transparency and accountability
A liveable and low carbon city: a destination of choice to live, visit, work	Not directly applicable
A connected city: world class infrastructure and connectivity to drive growth	Not directly applicable

**Contact Officers:**

Name: Fiona Ledden  
Position: City Solicitor  
Telephone: 0161 234 3087  
E-mail: f.ledden@manchester.gov.uk

Name: Jacqui Dennis  
Position: Deputy City Solicitor  
Telephone: 0161 234 3053  
E-mail: j.dennis@manchester.gov.uk

Name: Poornima Karkera  
Position: Head of Governance, City Solicitor's Department.  
Telephone: 0161 234 3719  
E-mail: p.karkera@manchester.gov.uk

**Background documents (available for public inspection):**

The following documents disclose important facts on which the report is based and have been relied upon in preparing the report. Copies of the background documents are available up to 4 years after the date of the meeting. If you would like a copy please contact one of the contact officers above.

Report to the Resources and Governance Scrutiny Committee dated 7 December 2017

## **1.0 Introduction**

- 1.1 The GDPR is the biggest change to Data Protection law in over 20 years. Although it derives from EU legislation its requirements have been incorporated into UK law by the Data Protection Act 2018. The GDPR came into force on 25 May 2018 and we are therefore in early days in terms of the new regime.

## **2.0 Background**

- 2.1 As indicated in the City Solicitor's report to this Committee in December 2017 whilst the fundamental principles of data protection remain largely unchanged, the GDPR introduces a much more enhanced data protection regime. At its core it brings a 21st century modernising approach to the processing of personal data in the digital age, imposing new obligations on data controllers, such as the Council (and for the first time) data processors (persons who handle information under outsourcing arrangements) as well as expanding the rights individuals have over the use of their personal information impacting people, processes and technology across all business functions.
- 2.2 A key change requires organisations not only to show compliance through existence of policies and procedures and staff training but to be able to demonstrate how in each case it has complied with GDPR requirements. It requires accountability at Board level evidencing a 'whole system' ethos in the way the organisation protects, governs and knows its data. The GDPR places increased requirements on data controllers such as the Council, e.g. requiring them to evidence everything from the legal basis for processing to the sharing of personal information (and all steps in between) and mandates that they evidence compliance, as well as requiring the adoption of a 'privacy by design' and 'privacy by default' approach.
- 2.3 The new legislation puts Data Controllers at risk of fines of up to 20 million euros if they fail to meet GDPR requirements. The Information Commissioner's Office (ICO) has other significant enforcement powers to deal with failure to comply with GDPR requirements e.g. temporary or permanent bans on processing personal data, and mandatory audits.

## **3.0 Main Issues**

- 3.1 To ensure that the Council is in a position to comply with the new data protection laws including the significant and necessary changes to processes, systems, policies, guidance, staff training etc. an intensive work programme led by an interdisciplinary team of officers has been carried out supported by a project manager. The project has been supported at a senior level across the Council with regular reporting to the City Solicitor who is the Council's Senior Information Risk Owner (SIRO), the Council's Corporate Information Assurance Risk Group (CIARG), Departmental SIROs (DSIROs) and the Council's Strategic Management Team (SMT).

- 3.2 Whilst there are areas where more work is needed to fully embed the new requirements the Council's rating using the ICO's data controller online GDPR self-assessment tool is 'overall green'. Work is being undertaken to draw up a plan in relation to Phase 2 of the GDPR project; to assist Directorate leads/ Deputy DSIROs (DDSIROs) ensure GDPR practices become embedded within the directorates.
- 3.3 The GDPR has introduced a new duty on all organisations to record all data breaches and to report data breaches that are likely to result in a risk to individuals to the ICO within 72 hours of becoming aware of the breach. If there is a high risk to the individual there is also a requirement to notify the individual without undue delay.
- 3.4 The Council's technical and organisational measures to mitigate loss of personal data include physical security measures such as building security and access controls, appropriate disposal of confidential waste, strong governance and oversight arrangements, appropriate policies, procedures and guidance notes and staff training and awareness. Technical measures include a number of best practice technologies and processes to ensure delivery of a robust and secure user environment.
- 3.5 The Council has built on existing practices and procedures to ensure staff are aware of the need to take care when handling personal data and what constitutes a data breach. The Council's data breach management procedures require managers and DSIROs / DDSIROs to risk assess data breaches and take urgent steps to contain the breach or otherwise mitigate the risks. Revisions have been made to procedures and guidance to reflect the new requirements and data breach handling has been devolved using a directorate based model. Awareness regarding GDPR requirements including data breaches has been raised by a variety of measures such as a 'Golden Rules' Comms campaign. 92% of staff with ICT access have completed the Council's IG e learning module (which takes into account GDPR). Arrangements have been made for training staff who do not have ICT access. Deputy DSIROs have received face to face training on data breach handling.
- 3.6 As required by GDPR the Council has appointed a Data Protection Officer (DPO). Broadly, the role of the DPO is to:
- provide advice and guidance to the organisation and its employees on the requirements of the GDPR
  - monitor the organisation's compliance with the GDPR and the Council's data protection policies including the assignment of responsibilities, awareness-raising, staff training and data audits
  - be consulted and provide advice during Data Protection Impact Assessments
  - co-operate with the ICO and act as the point of contact for the ICO on issues relating to data processing.
- 3.7 The Council's DPO is consulted in relation to all data breaches and as part of his role as officer responsible for monitoring data protection compliance makes recommendations to CIARG and DSIROs for actions to prevent

recurrence of specific categories of breach and to ensure lessons are learnt across the Council .

#### **4.0 Recommendations**

The recommendations appear at the front of this report.