Manchester City Council
Report for Information

Report to: Resources and Governance Scrutiny Committee – 7 December 2017

Subject: Update on General Data Protection Regulation (GDPR)

Report of: City Solicitor

Summary

To update the Committee on the work being undertaken to prepare for the coming into force in May 2018 of the General Data Protection Regulation (GDPR) which is the biggest change to data protection law in over 20 years.

Recommendation

The Committee is asked to note this report.

Wards Affected: all

Contact Officers:

Name: Liz Treacy
Position: City Solicitor
Telephone: 0161 234 3087
E-mail: l.treacy@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.

Information Matters Newsletters.

1. Introduction

1.1 The General Data Protection Regulation (GDPR) is the biggest change to data protection law in over 20 years. The regulation is EU law and will be coming into force automatically without the need for UK legislation on 25 May 2018. After a period of uncertainty following the Brexit decision it has become clear that compliance with the GDPR will be required notwithstanding the decision to leave the EU.

2. Background

2.1 Whilst the fundamental principles of data protection will remain largely unchanged, the new GDPR laws include a number of novel approaches and concepts, and will see the Data Protection Act 1998 repealed and replaced with a much more onerous regime. The GDPR places increased burdens 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 putting them at risk of much greater financial sanctions if they fail to meet the requirements (as well as other significant enforcement powers that will be available e.g. temporary or permanent bans on processing personal data, mandatory audits). Data protection compliance will become a much more significant issue for the Council, not least because failure to comply with the requirements of the GDPR can result in a maximum fine of up to 10 million euros with a fine of up to 20 million euros for a data breach.

2.2 To ensure that the Council will be 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 has been put in place, which requires support at a senior level across the Council.

3. Data Protection Reform – Background

3.1 The reform will be implemented under two instruments (as relevant to the Council):

(1) the EU General Data Protection Regulation ('GDPR') Regulation – which relates to personal data; and
(2) the Data Protection Directive ('DPD') Directive – which specifically relates to personal data in the police and criminal justice sector (which applies to the Council to the extent that it processes personal data for law enforcement purposes e.g. licensing and environmental health). This is being implemented through the recently published Data Protection Bill.

3.2 The GDPR will apply directly in the UK from 25 May 2018. The DPD must be transposed by the government into UK law by 6 May 2018. This report focuses on the GDPR.

4. What is new or different under GDPR?

4.1 While the GDPR has many similarities to the Data Protection Act (DPA) at its core it brings a 21st century modernising approach to the processing of personal data in the digital age, imposing new obligations on controllers (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.

4.2 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 will require accountability at Board level evidencing a 'whole system' ethos in the way the organisation protects, governs and knows its data. As indicated above fines for non compliance have been greatly increased. Further detail around the main differences between the DPA and the GDPR is provided at Appendix 1 to this report.

5. Work being undertaken to implement GDPR

5.1 GDPR briefing sessions have been carried out at Departmental Management teams to raise awareness and GDPR is a regular topic highlighted in the monthly information newsletter ' Information Matters' distributed to Heads of Service and available on the Council's Protecting Information intranet pages. GDPR discussions have taken place at Strategic Management Team to brief SMT, to ensure directorate engagement with data protection changes and discuss resourcing issues. Updates on GDPR preparation are provided as part of the Council's Annual Governance Statement. GDPR has also featured in ' The Buzz' (the Chief Executive's newsletter).

5.2 An interdisciplinary cross-departmental project team reporting to the Corporate Information Assurance Risk Group (CIARG) and to the City Solicitor as Senior Information Risk Owner (SIRO) for the Council has been set up to enable to Council to meet its obligations under the GDPR. The project team comprises 8 work streams covering the following areas – Policy and Governance, Data Subject Rights, Communications, Training, Information Collection & Sharing, ICT, Incident Breach Management and Records Management.

5.3 The workstreams draw on a number officers across the Council who have specialist data protection knowledge or other subject specialism. Membership of each workstream has been established following discussion with the Council's Directorate SIROs, the members of CIARG and validated by each workstream. Additional members are co-opted for specific items as needed. The workstreams generally meet monthly and workstream leads also meet monthly as a leadership group to discuss progress and key issues.

5.4 The project is supported by a full time Project Manager who attends workstream meetings and provides progress reports to CIARG and to the SIRO directly. AGMA colleagues meet to discuss common themes across Greater Manchester and officers attend and feed into these meetings.

5.5 A project plan to map, drive and take action to ensure delivery of each component of the project has been drawn up and work has commenced to understand more fully what personal information Council Departments holds by contacting officers who have been identified by DSIROs as Information Asset Owners within Directorates to facilitate the carrying out of an information audit so capture baseline information. A GDPR Risk register will be held by the City Solicitor. The Council will be required to appoint a Data Protection Officer (DPO) (see Appendix 1) and recruitment of a DPO is under way. Resourcing discussions are taking place at a senior level.

5.6 GDPR implementation will have some implications for Councillors as they are data controllers in relation to their constituency work and as this will affect all Councillors nationwide the Project group will work with AGMA to source appropriate training and materials for Councillors to ensure consistency with other councils.

6. Recommendation

6.1 The recommendation appears at the front of this report.

Appendix

What is new or different under GDPR?

Accountability, Compliance and Governance – a key change is the increased focus on accountability and governance.

Data controllers such as the Council will need to be able to demonstrate compliance with the data protection principles and this duty falls proactively (and promptly) on the data controller. Accountability requires the Data Controller not only to comply with the GDPR requirements but to evidence how it is complying. An assessment of the risks of noncompliance needs to be undertaken including the provisions that promote accountability (monitoring and review) and governance. As a data controller the Council needs to review what personal data it holds and any parties it shares the data with. Part of the overall governance focus is covered by the concepts of 'privacy by design' and 'privacy by default' this means appropriate technical and organisational measures should be built in to new projects which impacts on personal data from the outset.

There is also a legal requirement to carry out data protection impact assessments (DPIAs) if there are proposed activities likely to result in a high risk to the rights and freedoms of individuals. What 'high risk' means is not further expanded on as yet. DPIAs will consist of a range of questions on the activity including its objectives and outcomes as well as the scale of the data being processed, whether the new data is needed, what protections to privacy are being used and who might be effected and how if that protection fails. Detailed records of data processing must be kept and this will include DPIAs.

Consent to processing of personal data – this concept which derives from the DPA has been restated and revised so that there is now a requirement where consent is relied on to collect personal information for demonstrable consent by the individual (data subject). Consent in this context means clear affirmative action, and the consent should be informed, specific, unambiguous and freely given. Consent given, for example, in a contract will only be valid for the specific purposes set out in the contract. Consent is required for each purpose for which it is being processed, and explicit consent is still required for sensitive personal data. Under the GDPR satisfying the requirements around the consent route is far from easy. Individuals also have the right to withdraw their consent at any time

Enhanced rights of individuals – the rights of individuals as data subjects are strengthened and some new ones have been introduced:

- Right to be informed – there is an obligation to provide 'fair processing information' through privacy notices. There must be transparency at the point of collection on how the information will be used and there is an emphasis on clear, concise notices. The list of information to be provided in a privacy notice has been extended by the GDPR and includes for example an obligation to tell individuals for how long their information is being held.
- Right of access – individuals must be able to access their data to verify the lawfulness of the processing. This will continue to be through subject access

requests (SARs). The key change here however is the shortening of the time by which a response to a SAR is required to one month from 40 calendar days. The right to charge for a response has been removed except in exceptional circumstances.

- Right to be forgotten / of erasure or rectification– this right arises in the event of inaccurate or incomplete data and has been expanded to cover more circumstances than those set out in the current legislation.
- Right to data portability – this is a new right enabling individuals to reuse and transfer their personal data (held in electronic form) for their personal use to another data controller without restriction as it usability.
- Right to object – processing of personal data is subject to consent and individuals can object to certain types of processing such as direct marketing or processing for research or statistical purposes. Individuals must be given explicit notice of their right to object from the outset.

Data breach notification – a data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. The GDPR introduces a requirement to notify the relevant supervisory authority (in the UK the Information Commissioner's Office ('ICO')) of any data breach that is likely to result in a risk to the rights and freedoms of the individual affected. Notification at present is not mandatory. Failure to notify a breach is a breach of the GDPR itself. Where a breach occurs, it must be reported to the relevant supervisory authority without undue delay and within 72 hours of awareness**,** unless it is unlikely to result in a risk to the individuals. Any delay will need to be justified. Where there is a high risk the notification must be made to the individual as well. 'High risk' would include, for example, leaving the data subject open to discrimination, fraud or financial loss.

Enforcement – The fines that may be imposed for breaches of the GDPR have been significantly increased depending upon the type of breach, for the Council this could be a fine of up to 10 million euros for a simple failure to comply with the requirements of the GDPR or up to 20 million euros for a data breach.

Data Protection Officer - a Data Protection Officer ('DPO') who must report directly to the highest level of the organisation is a mandatory appointment. The DPO must be designated on the basis of appropriate professional qualities having an expert knowledge of data protection law. The DPO should also take responsibility for ensuring the Council complies with the GDPR.

Application – the GDPR applies more widely that the existing Data Protection Act 1998. For the first time, data processors will have direct obligations under the law (and any contracts with them will need updating).