Audit and Standards Committee Report

Report of: Acting Executive Director, Resources

Date: 27 April 2017

Subject: GENERAL DATA PROTECTION REGULATION (GDPR)

Author of Report: JOHN L CURTIS, HEAD OF INFORMATION MANAGEMENT, INFORMATION MANAGEMENT, BUSINESS CHANGE AND INFORMATION SOLUTIONS, RESOURCES

Summary:

This report outlines the proposed changes to how we process and use personal data.

These changes will be introduced through the General Data Protection Regulation (GDPR) which will come into force on May 25th 2018.

This report outlines some of the proposed changes outlined within the GDPR, as well as work undertaken to date and ongoing work to address these proposed changes.

Recommendations:

To note the proposed changes and support the ongoing work.

Background Papers:

Reference should be made to the Internet Links detailed within the report.

Category of Report: OPEN

Statutory and Council Policy Checklist

Financial Implications
NO
Legal Implications
YES
Equality of Opportunity Implications
NO
Tackling Health Inequalities Implications
NO
Human rights Implications
NO:
Environmental and Sustainability implications
NO
Economic impact
NO
Community safety implications
NO
Human resources implications
NO
Property implications
NO
Area(s) affected
None
Relevant Cabinet Portfolio Member
Councillor Ben Curran, Cabinet Member for Finance
Is the item a matter which is reserved for approval by the City Council?
NO
Press release
NO

GENERAL DATA PROTECTION REGULATION (GDPR)

1.0 INTRODUCTION

1.1 This report provides an overview of the proposed changes to Data Protection legislation which will be brought in through the General Data Protection Regulation (GDPR).

1.2 It also provides an overview of ongoing work around the project working group which has been established to support compliance in this area.

2.0 BACKGROUND

2.1 The European Union Commission proposed a General Data Protection Regulation in 2012, mainly to achieve the following objectives;

- Bring data privacy legislation up to speed with globalisation and technological advancements.
- Have a coherent approach to data privacy within Europe, all EU Member States following the same rules hence Regulation rather than a Directive.

2.2 The Regulation has been through various EU Authorities/Committees and was agreed fully and published in the Official Journal in May 2016.

2.3 It will come into effect in 25th May 2018 meaning we now have just over a year to be fully compliant. The current Data Protection Act 1998 will be repealed and replaced with local legislation where there is requirement and/or flexibility to enact local laws. Further information can be found at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

2.4 Although the UK plans to exit the EU, the Information Commissioner's Office (ICO) advice is that organisations within the UK should continue to work towards ensuring that they comply with the GDPR which becomes effective from May 2018.

2.5 It is important that we see this as an opportunity and should be used to get things right at the start when we collect and use (process) personal data. The GDPR is an opportunity to be much better placed around how we manage and process data, and reduce the recollection of the same personal data.

3.0 The main changes detailed within the GDPR are :

3.1 **Accountability**

The data controller (Sheffield City Council) is responsible for demonstrating compliance with the Regulation – this is not a new concept however the change is significant as this will be an explicit legal requirement under the GDPR. In addition, explicit compliance measures such as 'privacy by default' and 'privacy by design' are included in respect of development/application of technology/ policy.

In terms of documentation, Sheffield City Council as the data controller will be responsible for ensuring all processing activity records are kept including who its processors and joint data controllers are.

3.2 **New Rights for Individuals**

Data Portability, Sheffield City Council would need to have the ability to extract data that has been provided by the individual, in a format that can be easily transported /read by another provider/organisation

Restriction, individuals can ask Sheffield City Council to restrict data processing i.e. to contest legitimate ground unless verified by Sheffield City Council that such processing does not override data subject rights.

Profiling, when there are legal implications.

Right to be forgotten, this is a qualified right and has to meet certain conditions. It should be noted if the data is no longer required for the purposes it was collected for then this right applies. In any event data must be processed for specified purposes.

3.3 **New Types of Sensitive Data**

There are new types of sensitive data including genetic data, genetic characteristics of the individual, unique information resulting from an analysis of a biological sample.

Biometric Data, this includes facial recognition, finger prints etc.

3.4 **Fines**

Currently the maximum fine that the ICO can impose is £500,000. This will significantly change and will depend on the severity of the breach/ non-compliance/ notification. The maximum fine will be around £2m.

3.5 **Breaches**

Breaches are to be reported to the Supervisory Authority without undue delay and in any event within 72 hours. Failure to contain and notify would increase any fine unless there was good reason.

3.6 **Legitimate Interest of the data controller**

This is a new requirement of notification to the individual where processing is taking place under legitimate interest.

3.7 **Consent for processing data for children under 16 years of age**

Parental or holder of parental responsibility must consent if data is processed in relation to a minor. Some exemptions exist such as children's helplines etc. where consent is clearly irrelevant and not workable. **It should be stressed more than**

likely option of lowering this (to no lower than 13) by national derogation

3.8 **Data Protection Officer**

Appointment is mandatory for public authority or body, for data controllers that carry out systematic monitoring of individuals or if the activities consist of processing on a large scale of special categories of personal data. At this stage it is proposed that the Head of Information Management will take on this responsibility.

4.0 Ongoing work and Plan

4.1 Through the Information Governance Board and Working Group there is ongoing work through a dedicated GDPR project working group. We have also engaged with our insurer Zurich who will be providing some support. This has included a key note presentation in Sheffield from their IG lead (December 8th) and further development of a project / action plan.

4.2 Through the Yorkshire and Humber IG group the ICO also provided an update around the GDPR in Sheffield (January 20th).

4.3 To date communications have included Managers Brief (March 2017) and main coms updates are provided from the main GDPR page on the Council Intranet. http://intranet/ict/handling-council-info/info-governance/gdpr It is also proposed to also hold some drop in sessions around better use of data and GDPR so that we see this as an opportunity around how we manage this change. In addition, to this specific awareness sessions have been set up for elected Members and Schools (governors and head teachers).

4.4 A GDPR project working group has been established which includes members primarily from the Information Governance Working Group. Legal, and Commercial Services will specifically supporting interpretation of the regulation and work we need to do with SCC suppliers. A project plan has been created and signed off.

4.5 The first stage of this work will be a gap analysis (audit/ discovery phase) which will tease out what we need to do to become GDPR compliant. (reference should be made to the diagram at the end of this report which provides an overview of the methodology).

4.6 A sharepoint site has been established to support this work which also reuses previous IG audits we have undertaken across the council. For example, information sharing agreements, privacy impact assessments. The sharepoint site established will support work after the project and should greatly support our understanding of what data we hold, how it's been shared, and processed.

4.7 We do aim to ensure that this is seen as an opportunity to rationalise data collection, reduce the number of privacy notices we have and improve upon how we collect personal data once and then appropriately, safely and securely use many times.

4.8 By the end of this year it is proposed that anything identified as a "high risk" area (eg large volume of processing sensitive data) will have been assessed and controls put into place so

that we are compliant. This will include completion of a privacy/ data impact assessment. This is illustrated in the second part of the diagram.

5.0 RECOMMENDATIONS

To note the proposed changes and support the ongoing work.