To: **The Council**

On: **21 December 2017**

Report by: **Director of Finance and Resources**

Subject: **The EU General Data Protection Regulation**

1. **Summary**

1.1 The purpose of this report is to advise the Council of the new EU General Data Protection Regulation ("GDPR"), which will come into force on 25 May 2018, notwithstanding Brexit.

1.2 GDPR is the most significant data protection development in twenty years. This will mean important changes to existing data protection law and the way in which the Council addresses data protection compliance. As well as introducing new rights for individuals and enhancing existing rights, the monetary penalties for a data protection breach will increase from a maximum of £500,000 to 20 million Euro. The reputational damage for an organisation which fails to comply with GDPR will also be considerable.

1.3 Article 37 of the GDPR obliges the Council to designate a Data Protection Officer (DPO) on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. The key tasks of the DPO, which are prescribed by Article 39, are to inform and advise the Council 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) and to have due regard to the risk associated with the Council's processing operations.

The Managing Solicitor (Information Governance) has been appointed to this statutory role with effect from 15 November 2017 and section 4 of the scheme will be amended to reflect this. The title of the post has also been amended to Managing Solicitor (Data Protection Officer).

In addition to reflect the autonomy of this role, a new delegation has been added to section 5 of the scheme as follows:

"The Managing Solicitor (DPO) is authorised to discharge the role of statutory DPO, which includes autonomy in advising on all issues which involve the protection of personal data and monitoring compliance."

---

2. **Recommendations**

It is recommended that:-

2.1 The terms of the report, which detail the implications of GDPR for the Council, are noted;

2.2 The Council approve the implementation of the GDPR Action Plan summarised in paragraph 3.5;

2.3 It be noted that the Managing Solicitor (Data Protection Officer) has been appointed as Data Protection Officer;

2.4 Sections 4 and 5 of the scheme of delegated functions be amended to reflect this statutory appointment.

---

3. **Background**

3.1 The Data Protection Act 1998 came into force on 1 March 2000. This regulates how data controllers, such as the Council, process people's personal information. This is enforced by the Information Commissioner's Office (ICO).

3.2 On 25 May 2018, the law on data protection will change, as a result of GDPR. As the UK will still be a member of the EU on 25 May, GDPR will apply in full until the UK leaves. The Government has confirmed its

intention to bring GDPR into UK law post-Brexit through the Data Protection Bill, which is currently being debated in Parliament.

3.3 The Council needs to process personal information to operate. Failure to do this properly post May 2018, will not only expose the Council to higher monetary penalties and greater reputational damage, but will also reduce public confidence.

3.4 Although many of the key concepts and principles of GDPR are the same as the Data Protection Act 1998, some things are entirely new and some existing rights are enhanced. This means that the Council will need to do some things for the first time and some things differently.

Key GDPR changes will include:-

1. A duty to designate a statutory role of Data Protection Officer (DPO) with sufficient expertise, resources and the autonomy to perform the duties and tasks of the post in an independent manner;
2. An increase in monetary penalties from a maximum of £500,000 to 20 million Euro;
3. Mandatory, rather than voluntary self notification of any serious information security breaches to the ICO within 72 hours;
4. Increased data subject rights, including the need for more detailed privacy notices, changes to the right of erasure and the introduction of an entirely new right to data portability;
5. Reduction in the timescale for compliance with Subject Access Requests (SARs) from 40 calendar days to one calendar month;
6. Abolition of the £10 fee for SARs;
7. Stricter rules on consent, and
8. Privacy Impact Assessments (PIAs) become mandatory.

.

3.5 Although the Council already has a robust information governance framework, GDPR compliance will have resource implications, both in terms of preparatory work needed, in advance of May 2018 and ongoing compliance. It is of note that although the Information Governance Team within Legal and Democratic Services have always provided data protection advice and overseen compliance, the new statutory role of DPO extends beyond this with a specific monitoring role, as outlined at paragraph 1.3. The GDPR provides that the DPO should have a sufficient degree of autonomy and also explicitly

provides that an organisation must support its DPO by “providing resources necessary to carry out tasks and to access personal data and processing operations and to maintain his or her expert knowledge”.

The Team are leading the Council preparations, assisted by Service representatives on the Data Protection Working Group and the Information Management and Governance Group. ICT are also inputting to ensure that the Council has an up to date and fully functional Information Asset Register and that the Council’s systems are equipped to deal with new data subject rights, such as the right to data portability and right to erasure. These preparations form part of the Council’s GDPR Action Plan, which is based on the ICO’s guidance ‘Preparing for the Data Protection Regulation – 12 steps to take now’.

Those 12 steps include measures such as training and awareness raising, auditing and documenting information held by the Council, identifying the legal basis for processing information, thinking about how best to communicate privacy information to the public, considering how consent is sought, obtained and recorded and whether this will still be adequate under GDPR, ensuring that data breach management procedures are adequate, considering the impact of GDPR on both existing and new Council contracts, implementing relevant changes to processes and systems to comply with new rights of individuals and designation of a statutory Data Protection Officer (DPO).

All data protection and associated information governance procedures and guidance need to be revisited in early 2018. A revised Data Protection Policy will be submitted to Finance and Resources and Customer Services Policy Board in spring 2018 to reflect practical changes, which will take effect on 25 May, such as the abolition of the SAR fee and reduction in timescales.

GDPR training and awareness raising is being incorporated into the existing Information Governance Learning & Development Strategy and a communications plan is being developed to ensure that staff are aware of any changes which affect the way in which they work.

As well as processing personal information on the Council’s behalf, Councillors are also individual data controllers in their own right, in relation to information they process for constituents. A training session focusing on how GDPR will affect Elected Members has therefore been scheduled for 8 March 2018.

The Action Plan will be updated, as necessary, as further guidance becomes available from the ICO and the EU Article 29 Working Party.

3.6 Although the preparations for GDPR are resource intensive and the implications of this are highly significant for the Council, some of what is new is already being done by the Council as 'best practice', for example, conducting PIAs. Similarly, the Council already has procedures in place to manage any data breaches and those information security incident procedures will be of assistance in complying with the new obligation to self notify breaches to the ICO without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

Implications of the Report

1. **Financial** - The additional responsibilities on the Council under GDPR will result in a range of increased demands and risks to manage which will require additional support arrangements to operate across the Council. The financial implications of this will be incorporated into the budget planning arrangements for 2018/19.

2. **HR & Organisational Development –** HR & OD will assist with training in and awareness of GDPR by facilitating the launch of a GDPR specific iLearn module, prepared by the Information Governance Team, which will form the 2018 annual data protection refresher training.

3. **Community/Council Planning –**

- *Our Renfrewshire is thriving –* *enter details/ delete if not appropriate*
- *Our Renfrewshire is well -* *enter details/ delete if not appropriate*
- *Our Renfrewshire is fair -* *enter details/ delete if not appropriate*
- *Our Renfrewshire is safe -* *enter details/ delete if not appropriate*

- *Reshaping our place, our economy and our future -* *enter details/delete if not appropriate*
- *Building strong, safe and resilient communities -* *enter details/delete if not appropriate*
- *Tackling inequality, ensuring opportunities for all -* *enter details/delete if not appropriate*
- *Creating a sustainable Renfrewshire for all to enjoy -* *enter details/delete if not appropriate*
- *Working together to improve outcomes -* *enter details/delete if not appropriate*

4. **Legal** - GDPR is the most significant change to data protection legislation in twenty years and preparations are underway to ensure that the Council is compliant by 25 May 2018 when this comes into force. This has significant resource implications for the Information Governance Team, in particular.

5. **Property/Assets -** None

6. **Information Technology –** ICT are essential to the successful implementation of GDPR. As part of their information management function, they are leading on the updates to the Council's Information Asset Register and assessing the impact of new and enhanced data subject rights on ICT systems.

7. **Equality & Human Rights** -

(a) The Recommendations contained within this report have been assessed in relation to their impact on equalities and human rights. No negative impacts on equality groups or potential for infringement of individuals' human rights have been identified arising from the recommendations contained in the report because it is for noting only and GDPR will increase information rights. If required following implementation, the actual impact of the recommendations and the mitigating actions will be reviewed and monitored, and the results of the assessment will be published on the Council's website.

8. **Health & Safety -** None

9. **Procurement –** Provision now needs to be made for GDPR in Council contracts, as appropriate.

10. **Risk-** GDPR compliance is addressed on the Council's corporate risk register to ensure that key milestones are met and the Council is fully compliant by May 2018.

11. **Privacy Impact –** Privacy Impact Assessments (PIAs) are currently conducted, as best practice, by the Council in relation to projects or initiatives which involve processing personal information in new ways and have a potential privacy impact. PIAs will be mandatory when GDPR comes into force on 25 May 2018.

12. **Cosla Policy Position –** Not applicable

List of Background Papers

(a) Background Papers - None

Author **Allison Black, Managing Solicitor (DPO), extension 7175**