REPORT TO:	**COUNCIL**	**AGENDA ITEM: 11**
DATE OF MEETING:	**12th APRIL 2018**	**CATEGORY: RECOMMENDED**
REPORT FROM:	**STRATEGIC DIRECTOR CORPORATE RESOURCES**	**OPEN**
MEMBERS' CONTACT POINT:	**KEVIN STACKHOUSE (01283 595811)** Kevin.stackhouse@south-derbys.gov.uk	**DOC:** u/ks/data security/GDPR/GDPR report to council 12th April 2018
SUBJECT:	**THE GENERAL DATA PROTECTION REGULATION 2018**	**REF**
WARD (S) AFFECTED:	**ALL**	**TERMS OF REFERENCE:**

1.0 Recommendations

1.1 That the requirements placed on the Council arising from the General Data Protection Regulation 2018 are noted.

1.2 That the Council's ICT and Business Change Manager is appointed as the Council's Data Protection Officer from 25th May 2018 under Article 39 of the General Data Protection Regulation 2018.

1.3 That the implications for the terms and conditions of that Post (in 1.2 above) are subject to the Council's Job Evaluation Scheme.

2.0 Purpose of Report

2.1 To outline the requirements of the General Data Protection Regulation (GDPR) 2018 that will come into force on 25th May 2018. This includes a recommendation regarding the appointment of a Data Protection Officer (DPO) under the Regulation.

3.0 Detail

3.1 The EU General Data Protection Regulation (GDPR) was implemented in May 2016 and will apply in the UK on 25 May 2018 after a two-year transition period. It is expected that following "Brexit" the UK Government will still implement the GDPR.

3.2 Generally, the GDPR principles are much the same as those in the current Data Protection Act which has existed since 1988. The primary objectives of the GDPR are to give citizens greater control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

3.3 As a processor of personal data, the Council has an obligation to properly process and manage personal information and to keep it secure. The GDPR will therefore apply to the Council.

3.4 The key changes within the GDPR include:

- Regulators can impose fines for non-compliance of up to 4% of annual turnover or 20 million Euros.
- A Data Protection Officer must be formally designated and appointed by an organisation.
- Organisations must demonstrate that data protection is embedded by documenting data protection procedures, building it into system processing and minimising data retention.
- Privacy Impact Assessments must be conducted for large scale processing of personal data.
- Consent to process data must be freely given, explicit and individuals must be informed of their right to withdraw their consent.
- Organisations must inform the regulatory body (normally the Information Commissioner) of data breaches without undue delay or within 72 hours, unless the breach is unlikely to be a risk to individuals.
- Enhancement of new rights – the right to be forgotten, the right to data portability and the right to object to profiling.

3.5 Privacy Impact Assessments are only required for new systems or where data is being collected for specific purposes. Together with the new rights of individuals, it is considered that this will place an additional burden upon organisations.

Impact on the Council

3.6 As a public body, the Council has established policies and procedures in place regarding data protection and the principles are generally embedded within the organisation. The Council's position ahead of the introduction of the GDPR has been reviewed independently and a work programme is being progressed.

3.7 Overall compliance with the GDPR is a key action within the Council's Governance Work Programme for 2018/19 and this is being monitored by the Audit Sub-Committee. Key actions progressed are:

- Policies regarding Records Management and Document Retention have been reviewed and updated where necessary.
- Document retention schedules have been reviewed and updated.
- An information audit and data cleansing exercise is currently taking place.

- A review of contracts and relationships with third parties, for example financial vendors, is being progressed.

- A communications plan is being implemented which is raising awareness with employees through regular briefings.

- Policies and registers relating to CCTV are being updated.

- Standard documentation is being put in place for dealing with subject access requests and for recording data breaches. New request forms for dealing with privacy impact assessments and the new rights for individuals are to be drawn up.

3.8 When all work has been completed, any necessary changes to the overarching Data Protection and Information Security Policies will be made.

Mandatory Data Protection Officer (DPO)

3.9 A new requirement under the GDPR is that the Council must designate one of its officers as the DPO. Under the 1988 Data Protection Act, this role is currently fulfilled by the Strategic Director of Corporate Resources.

3.10 Under the 2018 GDPR, the role must be independent of the senior management team of an organisation. The GDPR does not set out any precise credentials a DPO should have, only that they should have professional knowledge of data protection law and this should be proportionate to each organisation.

3.11 The appointment should be determined according to the data processing operations carried out locally. If the post is to form part of the duties of an existing employee, ideally it should complement those duties and responsibilities. Given this, it is proposed that the role of the DPO is assigned to the Council's ICT and Business Change Manager.

3.12 A current part of this role is to ensure that electronic data is processed securely and is safeguarded. The role also acts as the Council's lead on IT data security and associated policies. The role also has a corporate input into service improvement and is well placed to consider data processing at that stage.

3.13 Therefore, it is considered that there is some synergy with the wider role of the DPO.

3.14 Article 39 of the GDPR defines the minimum tasks of a DPO. These include:

- To inform and advise the organisation and its employees about their compliance obligations.

- To monitor compliance with the GDPR and ensure that proper arrangements are in place.

- To be the first point of contact for regulators, together with other public agencies regarding data sharing protocols.

3.15 The DPO has to report to the highest management level in an organisation to raise compliance issues and should be informed of data processing matters emanating from policy and service development.

3.16 If the proposal to appoint the ICT and Business Change Manager as the Council's DPO is approved, it is recommended that any impact on the current terms and conditions of the current post holder are considered through the Job Evaluation Scheme.

3.17 Consultation and additional training will also be provided to the current post holder.

4.0 Financial and Corporate Implications

4.1 None arising direct from this report.

4.2 However, it was highlighted previously that a significant fine could now be incurred for Personal Data Breaches. These are defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4.3 In order to avoid penalties, it is important that the Council continues to adopt robust procedures to protect personal data, not only through its life, but right to the point of its disposal.

5.0 Community Implications

5.1 The implementation of the GDPR is to give local residents greater control of their personal data.

6.0 Background Papers

6.1 Guidance notes issued by the Information Commissioner's Officer at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/