POLICY, RESOURCES & GROWTH COMMITTEE	Agenda Item 71 Brighton & Hove City Council

Subject:		**Response to General Data Protection Regulation**
Date of Meeting:		**30th November 2017**
Report of:		**Executive Director, Finance & Resources**
Contact Officer:	**Name:**	**Peter Bode** **Tel: 01273 29 6634**
	Email:	**Peter.bode@brighton-hove.gcsx.gov.uk**
Ward(s) affected:		**All**

FOR GENERAL RELEASE

1. PURPOSE OF REPORT AND POLICY CONTEXT

1.1 The purpose of this report is to inform the Committee of the forthcoming changes to Data Protection regulations, the impact these will have on the Council's operations, and the proposed approach to mitigating the associated risks. At the heart of this is the General Data Protection Regulation (GDPR) which comes into effect in May 2018.

1.2 The approach has been devised by the Council's Information Governance Team in collaboration with and benchmarked against that of our Orbis colleagues in East Sussex.

1.3 As the report demonstrates there will undoubtedly be significant financial implications – hence the reason for bringing GDPR to the Committee's attention – but in the longer term, the council will seek to ensure that these costs are reduced, as meeting the new requirements will need to become a part of 'business as usual'.

2. RECOMMENDATIONS:

That the Committee:

2.1 Approves the preferred option of a 'Hub and Spoke' model to ensure that accountability for successful compliance with the forthcoming GDPR and UK Data Protection Bill 2017 is in place.

2.2 Approves capital funding for 2017/18 and 2018/19 of up to £644,000 and the commitment of £90,000 per annum from 2019/20 in the revenue budget – these costs are to cover investment in Information Asset Administrator employment, software development, and project management resources as detailed within the options appraisal and business case in Annex A.

2.3 Delegates authority to the Executive Director of Finance and Resources to take all steps necessary to implement the GDPR strategy.

3. CONTEXT/ BACKGROUND INFORMATION

3.1 The GDPR has direct application throughout the EU and member states are required to comply with it from 25th May 2018. The Data Protection Bill 2017, which is currently before the UK Parliament, effectively extends GDPR principles to general data processed both within the UK and between the UK and other countries, regardless of whether or not they are EU member states. It also transposes the Law Enforcement Directive into UK law, thereby regulating the processing of personal data for the purposes of crime prevention.

3.2 While in many ways the new regime builds on existing data protection law, it will bring with it amongst other things:

- Broader personal information rights, including an enhanced ability to object to processing and a new right to be forgotten as well as a more robust regime in relation to data breaches.

- A requirement to be explicitly transparent about what the data that organisations collect about citizens will be used for, how it will be maintained, and who it will be shared with.

- Enhanced regulatory powers for the Information Commissioner's Office (ICO) including a revision of the fines regime from its current ceiling of £500,000 to a maximum of €20,000,000 (converted to £sterling).

3.3 The GDPR is extensive and comprises 99 articles (or requirements). Central government has indicated that the new data protection regime will not be altered by the UK leaving the EU. We can reasonably expect the draft UK bill referred to in paragraph 3.1 above to pass without significant amendments in order to provide certainty to the UK business sector.

3.4 Compliance with the new Regulation and the forthcoming Act will require the council to review its approach to data processing across all of its functions. The following actions are required:

i. Conduct an audit to review and refine our understanding of and justification for the personal data we hold, its legal basis for processing, and the impact it may have on the privacy of individuals

ii. Analyse, improve and reduce the personally identifiable data we hold, reflecting stricter obligations for accuracy, adequacy and relevance of the data

iii. Introduce new measures for transparency about how data is used

iv. Implement and monitor new safeguards for information sharing with partners and commissioned organisations

v. Implement improved business process and information design in existing and new corporate systems, amongst other things to ensure that the Council adheres to the 'privacy by default' expectation and applies the required 'privacy by design' approach

vi. Embedding changes to contract and procurement processes where personal data is involved

vii. Implement reduced legal timeframes for responses to Subject Access Requests, in relation to which a fee will not normally now be chargeable

viii. Comply with the mandatory requirement to designate a Data Protection Officer, and to meet the new Data Protection principle which requires the organisation to demonstrate compliance via appropriate policies and processes

3.5 The regulatory change will require the council to both prepare for the start of enforcement next year, and also to also build compliance into ongoing operations, changes to corporate structure, engagement with external partners and procurement/development of new systems. It is worth noting that the council's strategic approach to shared service delivery and integration with city partners creates heightened risk to both individual privacy and therefore to the council if the challenges posed by the GDPR are not addressed.

3.6 Conversely, the GDPR should not be seen as merely a compliance imposition. The required improvements to data quality and business processes offer the opportunity to improve interactions with residents, improve cross-council collaboration opportunities, open up digital service delivery channels, and avoid information management costs in the future.

3.7 The council's Audit & Standards Committee and Modernisation Member Oversight Group have recently received reports on how the council is improving its approach to managing all risks relating to Information Governance. In order to ensure that there is ongoing strong governance in this area, these forums will receive regular updates from a newly formed GDPR Programme Board to ensure that progress is scrutinised and challenged. This Board will be chaired by the Executive Director, Finance & Resources.

3.8 Regarding the DPO post (paragraph 3.4 – viii) options for recruiting the DPO post are being explored. It may be that the strongest candidate will be available if a joint-Orbis appointment is made, however further consultation is required before a decision can be taken. As well as being statutory, the role assures GDPR is delivery by:

a. informing the council around its data processing and information governance activities, and facilitating compliance with the GDPR and other UK data protection law,

b. Monitoring compliance with GDPR, other UK law and with SCC policies in relation to the protection of personal data – including assignment of responsibilities, training, and awareness raising of staff. To monitor compliance with any related audits against GDPR requirements.

c. Providing expert advice in all matters relating to data protection impact assessments (DPIAs) the monitoring of the council's performance in

relation to data processing, and consultation with the ICO prior to data processing where a DPIA indicates that processing would result in a high risk in the absence of measures taken to mitigate the risk.

d. Acting as the key contact point for, the ICO on any issues relating to data processing.

3.9 The DPO and stronger governance are central to improving risk management over information, an area where the historic performance of the council has been mixed. Although the financial penalties are known (paragraph 3.2) it is not yet clear how robust the ICO will be. Recent intelligence is that what must be achieved quickly is a detailed awareness of how the GDPR affects the council, and a demonstration that a clear plan is in place and under way by May 2018.

3.10 Below is a clear recommendation for the approach – however the detail will evolve as the programme moves forwards, and more is understood, for example the direction of travel from the ICO. The delegation sought by recommendation 2.3 is therefore key, as the council needs to make as much progress as possible as soon as possible.

4. ANALYSIS & CONSIDERATION OF ANY ALTERNATIVE OPTIONS

4.1 A full options appraisal is included in Annex A. In summary, the options considered were as follows.

4.2 **Option 1: Aim to achieve compliance with existing IG staff resource.**

This option is not recommended on the basis that it is considered highly likely to attract attention from the regulator, including the prospect of substantially increased fines. It is also likely to increase exposure to civil litigation.

4.3 **Option 2: Adopt a Hub and Spoke model.**

Project Management resource and legislation/analysis expertise will reside in the corporate centre (IT & Digital and Legal with support from Performance Improvement & Programmes) while information asset expertise within each service will carry out analysis and recommend/carry out the required changes within services, while locally, experts in the business processes and use of information will liaise with the central resource whenever business changes impact on how personal information is to be kept or used.

The project will seek opportunities to share tools and techniques (and potentially resources) with partner organisations such as Orbis. It is not anticipated that external consultancy will be required.

4.4 **Option 3: Create a small centralised team within IT&D to manage the project and ongoing compliance.**

This option fails to recognise that the GDPR impacts on all service areas and the implications of that cannot be successfully managed from a team centralised in a single area.

4.5 The recommended and preferred option is **Option 2** - a Hub and Spoke model which will deliver compliance through the implementation of an Information Asset Ownership Framework across all areas of the Council. This is expected to deliver enduring benefits in terms of quality and cost avoidance.

5. COMMUNITY ENGAGEMENT & CONSULTATION

5.1 Impacted stakeholders include residents, staff, commissioned service delivery partners, our Orbis colleagues and other local government agencies such as the Sussex Police and NHS Trusts.

5.2 To date, consultation has been largely informal, pending approval of a GDPR Strategy for the Council.

6. CONCLUSION

6.1 The recommended option will develop corporate information management maturity across the Council, improving the economics of information and reducing opportunity cost

6.2 The Audit & Standards Committee will oversee the implementation of this work, both to provide Member oversight and as a demonstration of compliance with the new data protection principles.

6.3 The benefits of the option will extend to safer handling of resident information, avoiding fines, civil penalties, whilst having a positive impact on community perception of the Council as a trusted data custodian.

6.4 The proposal aligns with those being undertaken at our Orbis partners, introducing ongoing opportunities for knowledge sharing, collaboration and (potentially) integration of information technology and digital services over time.

7. FINANCIAL & OTHER IMPLICATIONS:

Financial Implications:

7.1 The preferred option of a Hub and Spoke approach to meet the forthcoming GDPR and UK Data Protection Bill 2017 requirements is estimated to cost £914,000 over the next 4 years. This includes £644,000 of capital costs and ongoing revenue costs from 2019/20 of £90,000 per annum, £270,000 over the 4 year period. The capital costs will be funded from unallocated capital receipts. The Budget Update report to this committee in July 2017 highlighted there was £7.5m unallocated receipts; subsequently, this committee allocated £2.5m of this funding for the replacement of the current Care First system. This means there is £5.0m unallocated subject to recommendations elsewhere on this agenda. The ongoing revenue costs of £90,000 will be treated as a commitment in the Medium Term financial Strategy from 2019/20 onwards.

7.2 The implementation of the preferred option is expected to reduce the volume of data held by the council and this could lead to ongoing savings although at this

stage, these are unquantifiable. A range of non-cashable benefits is included in appendix 1 along with the breakdown of expected costs.

Finance Officer Consulted: James Hengeveld *Date: 20/11/17*

Legal Implications:

7.3 The deadline for compliance with the GDPR (which applies directly in the UK) is 25th May 2018. The draft Data Protection Bill (which is expected to come into force well before that) both transposes the Law Enforcement Directive into UK law and includes some derogations to the GDPR. It furthermore extends the new data protection regime by requiring compliance where general data is processed either within the UK or outside it (ie whether or not EU citizens are impacted). This Report highlights some of the requirements which need to be met and the actions which need to be undertaken in order to comply with the new data protection regime and to meet the new accountability principle. In the context of an enhanced and more robust regulatory regime where the risk of legal challenges to the Council's processing of personal data is increased, this Report proposes a recommended model for addressing the challenges.

Lawyer Consulted: Victoria Simpson *Date: 14/11/17*

Equalities Implications:

7.4 It is not judged that an Equalities Impact Assessment needs to be conducted for this project. However, there are requirements around the rights of data subjects which will require EIAs to be completed when making arrangements and drawing up work processes for dealing with the following:

- Informed Consent
- Right to Erasure
- Right to Object
- Right to Restrict Processing
- Right to withdraw consent
- Right to rectification

7.5 There will be a need for an EIA for informed consent, as the project will deal with issues around informed consent and the understanding of this may vary for different groups in the community, relating to their protected characteristics. This should also help to engage the audience with the need for investment.

Sustainability Implications:

7.5 Not Applicable

SUPPORTING DOCUMENTATION

Appendices:

1. GDPR Full Business Case

Documents in Members' Rooms

1. None

Background Documents

1. None