Report to:	**Governance Committee**
Date of meeting:	**24 April 2018**
By:	**Chief Operating Officer**
Title:	**Data Protection Officer designation required by the General Data Protection Regulation**
Purpose:	**To consider proposals which are a means of ensuring compliance with the General Data Protection Regulation**

RECOMMENDATIONS

The Governance Committee is recommended to recommend the County Council to:

1. approve the Council having a single shared designated statutory Data Protection Officer with Brighton & Hove City Council and Surrey County Council;

2. delegate authority to the Chief Operating Officer, in consultation with the Chief Executive, to appoint or designate to the role of statutory Data Protection Officer; and

3. delegate authority to the Assistant Chief Executive to amend the Council's Constitution where necessary so as to give effect to this decision and to include provision in the Scheme of Delegations to Officers for the new statutory Data Protection Officer role.

1 Background

1.1 Article 38 of the General Data Protection Regulation (which is directly applicable in the UK) imposes a mandatory requirement that all public authorities designate a Data Protection Officer ('the DPO'). It provides that 'the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39'.

1.2 The DPO's details must be published, and – although they may be an employee or contractor – they must be supported in carrying out their roles and responsibilities, which are to be executed with independence. The DPO may not be dismissed or penalised for carrying out his or her tasks and must report to the highest management level regarding the detailed range of tasks indicated in article 39. These include providing advice on the lawful performance of the Council's obligations and monitoring its compliance as well as assisting in the assignment of responsibilities and in relation to data protection impact assessments and acting as contact point with the Information Commissioner's Office ('the ICO').

1.3 The term 'Data Protection Officer' has been in common use in local government for some time and has historically been used to describe those officers who deal with subject access requests made under the Data Protection Act 1988. However this statutory role is a new requirement for local authorities (and indeed most organisations) and is to be distinguished from that.

1.4 Article 38 of the GDPR specifically permits a single Data Protection Officer to be designated for several public bodies or authorities. This has been actively explored as an option by this Council in discussion at officer level with its fellow Orbis partners, Surrey County Council and Brighton & Hove City Council. The increasing alignment of relevant support services including Audit – an alignment which is obviously a key feature of the Orbis project - has informed these proposals. They will offer this Council access to an individual with dedicated expertise and seniority, this via a model which as well as satisfying a key GDPR requirement offers the potential to positively influence the work done by the sovereign Information Governance function, including meeting the need to ensure compliance in terms of our arrangements across Orbis for sharing information.

1.5 It is proposed the funding for the joint DPO appointment will be agreed by the Orbis Joint Management Board and will reflect an appropriate methodology which is governed by the relative information maturity of the three authorities. There is no bid for funding additional to that which has already been agreed.

1.6 This proposal is considered to offer a solution which complies with the requirements of the GDPR in such a way as to inform and benefit this authority's approach to its information governance arrangements. The shared DPO's independence will be reinforced by the basis on which they are appointed (ie across the three authorities) and they will moreover be well-placed amongst other things to identify opportunities for any joint work streams which arise while ensuring that their main focus is on deploying their skills, experience and seniority to discharge their statutory functions.

2 Supporting information

2.1 It is considered by the ICO to be good practice for councils to appoint a Senior Information Risk Owner (SIRO) to ensure accountability and effective risk management in relation to information held across the range of the authority's functions. Although this is a non-statutory role, it is considered to be key to ensuring that one of the Council's Chief Officers retains responsibility for maintaining oversight of the Council's ongoing (and continually evolving) use of technology to deliver its functions.

2.2 Currently the SIRO role is fulfilled by this Council's Chief Operating Officer. It is proposed that this arrangement continues.

2.3 Compliance with the requirements of the General Data Protection Regulation is mandatory and – while different models exist for ensuring compliance with the requirement to designate a DPO – the proposals outlined here are recommended.

3 Conclusion and recommendations

3.1 The Committee is asked to recommend to the County Council to agree to having a single shared statutory Data Protection Officer with Brighton & Hove Coty Council and Surrey County Council; to delegate authority to the Chief Operating Officer, in consultation with the Chief Executive, to appoint to or designate that role, although the person appointed will be the statutory office for the Council they may be an employee of one of the other Councils; and to delegate authority to the Assistant Chief Executive to amend the Council's constitution accordingly.

KEVIN FOSTER

Chief Operating Officer

Tel: 01273 481412

Email: kevin.foster@eastsussex.gov.uk

Local Member: All

Background Documents: General Data Protection Regulations