



INTEGRATION JOINT BOARD

Report Title	Data Protection Officer
Lead Officer	Alex Stephen, Chief Finance Officer, ACHSCP
Report Author (Job Title, Organisation)	Alan Thomson, Solicitor, Aberdeen City Council
Report Number	HSCP/18/037
Date of Report	27 April 2018
Date of Meeting	22 May 2018

1: Purpose of the Report

1.1 To advise the Integration Joint Board of the requirement to appoint a Data Protection Officer.

2: Summary of Key Information

2.1 The new General Data Protection Regulation (GDPR) comes into effect on the 25th May 2018.

- The GDPR introduces a duty for public authorities to appoint a data protection officer (DPO).
- DPOs monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases, several organisations can appoint a single DPO between them.
- DPOs can help demonstrate compliance and are part of the enhanced focus on accountability.

2.2 The DPO's tasks are defined in Article 39 as:

- to inform and advise the IJB about obligations to comply with the GDPR and other data protection laws;



INTEGRATION JOINT BOARD

- to monitor compliance with the GDPR and other data protection laws, and with data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

2.3 It's important to remember that the DPO's tasks should also cover all personal data processing activities, not just those that require their appointment under Article 37(1).

- When carrying out their tasks the DPO is required to take into account the risk associated with the processing undertaken. They must have regard to the nature, scope, context and purposes of the processing.
- The DPO should prioritise and focus on the riskier activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to your organisation.
- If the IJB decide not to follow the advice given by their DPO, the reasons for not doing so should be documented to help demonstrate accountability.



2.4 The Data Protection Bill will define what a 'public authority' is under GDPR. This is likely to be the same as those defined under the Freedom of Information Act (Scotland) 2002 which includes the IJB. However, the Data Protection Bill is subject to amendment and officers will confirm the IJBs status when the Bill becomes an Act of Parliament.

2.5 The IJB is not expected to have much personal data. This is because the partners are responsible for operational delivery of the functions and services. Therefore, the partners will be the data controllers, either separately or jointly, for all the services delivered by Partnership. The IJB will have some data controller responsibilities for reports it receives, complaints to the Board, information about seconded staff, and other small amounts of data. The DPO for the IJB is, therefore, not expected to have much to do for the IJB. It is hoped that one of the Partner's DPO's will take on responsibility for the IJB. Any costs associated with the appointment are likely to be minimal.

2.6 Aberdeen City Council's (ACC) DPO is currently the Chief Officer – Governance. This may change once the new organisational structure has been finalised later this year. The DPO for NHS Grampian (NHSG) is the Information Governance Lead.



INTEGRATION JOINT BOARD

3: Equalities, Financial, Workforce and Other Implications	
<p>Equalities – Not applicable</p> <p>Financial – There is no or minimal anticipated cost to providing this service to the IJB due to the small amount of work anticipated for the IJB.</p> <p>Workforce – While all NHS staff and ACC staff must all comply with GDPR this is already being done by the individual DPOs for both organisations.</p> <p>Other – Not applicable</p>	
4: Management of Risk	
If the IJB does not appoint a Data Protection Officer, it will be in breach of new data protection legislation.	
5: Recommendations	
<p>It is recommended that the Integration Joint Board:</p> <ol style="list-style-type: none">1. Approve the appointment of a Data Protection Officer for the Integration Joint Board and instruct the Chief Officer to make the necessary arrangements with the relevant Partner.	
6: Signatures	
	Sally Shaw (Interim Chief Officer)
	Alex Stephen (Chief Finance Officer)