General Medical Council

Agenda item:	**12**
Report title:	**GDPR – Data Protection Officer Appointment**
Report by:	**Neil Roberts**, Director of Resources and Quality Assurance, Neil.roberts@gmc-uk.org, 0161 923 6230
Action:	**To note**

Executive summary

The General Data Protection Regulation (GDPR) comes into force in the UK on 25 May 2018. By that date, the GMC will be required to have a mandatory Data Protection Officer (DPO) in place.

The GDPR sets out the requirements for the DPO post and the mandatory tasks that the DPO must fulfil. Guidelines have been issued by the Article 29 Working Party (the group made up of data protection regulatory authorities across Europe) providing further detail.

Recommendations

The Executive Board is asked to note:

a The appointment of Andrew Ledgard as the GMC's Data Protection Officer.

b That the DPO reports to the GMC's senior management and, if appropriate, the ARC on matters relating to compliance with the GDPR.

The role of the DPO

1 The DPO should be designated on the basis of professional qualities, in particular "*expert knowledge of data protection law and practices*"*[*]

2 The official guidelines suggest that the DPO should have:

- Expertise in national and European data protection laws and an in-depth understanding of the GDPR.
- Knowledge of the business sector and of the organisation itself.
- Sufficient understanding of the processing operations, information systems, data security and data protection needs of the organisation.
- Sound knowledge of the administrative rules and procedures of the organisation.

3 The DPO is the cornerstone of accountability, and will facilitate compliance with the GDPR acting as the intermediary between all of the relevant stakeholders (data subjects, the Information Commissioner's Office and the different business units within the GMC).

4 The Guidelines envisage that the DPO is involved in a very hands-on way with day to day data protection compliance: "The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing, and notification and communication of data breaches."

5 The DPO[1]:

- Must be involved in a timely manner in all issues that relate to data protection.
- Must be supported by the organisation by the provision of appropriate resources to carry out his/her tasks and maintain expert knowledge.
- Does not receive any instructions regarding how to carry out tasks (i.e. has a sufficient degree of autonomy/independence).
- Shall not be dismissed or penalised for fulfilling his/her tasks.

[*] GDPR Article 37(5)

- Shall report directly to the highest management level of the organisation.

6 The requirement for the DPO to report directly to the highest management level of the GMC does not extend to the line management of the DPO, but can be met by the DPO having an appropriate and effective means for reporting to SMT/the Executive. The DPO may also provide reports to Audit and Risk Committee if deemed appropriate.

7 The mandatory tasks for the DPO are to:

- Be involved in all issues which relate to processing of personal data (which would include for example information security incidents/data breaches).
- Inform and advise the organisation and its employees of their obligations under the GDPR and UK data protection laws.
- Monitor compliance with the GDPR and UK data protection law.
- Monitor compliance with the GMC's policies in relation to the protection of personal data, including assignment of responsibilities, awareness-raising and training of staff, and related audits.
- Provide advice regarding Data Protection Impact Assessments and monitoring their performance in compliance with Article 35.
- Co-operate with the Information Commissioner.
- Act as contact point for Information Commissioner including statutory prior consultation.

Conflict of interests

8 The DPO may fulfil other tasks duties, but those should not result in a conflict of interests with their role as DPO, for example, the DPO should not be in a position where they are providing data protection compliance input into an area over which they have operational responsibility. The Guidelines suggest that conflicting positions might include those such as Chief Executive, Chief Operating Officer, Head of IT etc.).

Dismissal or disciplinary action for performing DPO tasks

9 Penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. The DPO may still be disciplined or dismissed legitimately for reasons other than performing their DPO tasks, just as any other employee.

Recommendation for appointment of DPO

10 By virtue of his position, expertise and experience, Andrew Ledgard meets the DPO criteria set out in the GDPR guidelines.

Recommendation for reporting by the DPO

11 The DPO provides an annual report to the Executive Board covering all areas of data protection compliance under the GDPR.

12 Exception reporting of significant data breaches or high risk data protection compliance concerns will be reported by the DPO to the Senior Management Team (and if appropriate the ARC) as and when required.

General Medical Council

12 – GDPR – Data Protection Officer appointment

12 – Annex A

GDPR Articles relating to the DPO

GDPR Articles: Section 4 Data protection officer

Article 37 Designation of the data protection officer

1 The controller and the processor shall designate a data protection officer in any case where:

a the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2 A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3 Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4 In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5 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.

6 The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7 The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38: Position of the data protection officer

1 The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2 The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3 The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4 Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5 The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6 The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39: Tasks of the data protection officer

1 The data protection officer shall have at least the following tasks:

a to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

b to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

d to cooperate with the supervisory authority;

e to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2 The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.