General Medical Council

Agenda item:	**9**
Report title:	**Annual Report of the Data Protection Officer**
Report by:	**Andrew Ledgard**, Head of Information Policy, Resources. Andrew.ledgard@gmc-uk.org, 020 7189 5418
Action:	**To note**

Executive summary

The GMC successfully implemented the requirements of the General Data Protection Regulation, overseen by a cross-cutting programme board. We have seen an increase in the volume of subject access requests received by the organisation as well as requests to rectify or erase personal data. We have not experienced any information security breaches which require formal notification to the Information Commissioner's Office.

Recommendation

To note the Data Protection Officer's Annual report.

GDPR Implementation in 2018

1 The GMC undertook a programme of work during 2017 and 2018 to implement the General Data Protection Regulation (GDPR). This officially went live on 25 May 2018. The programme impacted the entire organisation and was overseen by a cross-cutting programme board with representation from across the GMC and MPTS.

2 Prior to go-live we undertook a readiness review. This was largely positive and noted that our implementation could be used as a benchmark for other organisations. Of particular note was the review's recognition of our internal communications activities and revised training materials. Some highlights of the programme are provided below.

3 During the course of the programme, Procurement colleagues undertook a major review of our existing contracts. We updated these to reflect the new obligations imposed by the GDPR. In particular, we were obliged to officially designate our commercial partners as data controllers, data processors or neither. This was a sizeable undertaking and required lengthy discussions with third party suppliers.

4 The GDPR requires public authorities to rely on their statutory functions as their legal basis for processing personal data. This meant we were unable to rely on data subject consent as our "processing condition". This had a huge implication for the way we do business. For example, Fitness to Practise colleagues traditionally placed consent at the heart of their processes and we were required to construct a new approach to reflect the new GDPR requirements. This involved establishing a large team to revise several hundred template documents, develop new policies and procedures as well as provide training for staff. We achieved this on time with extensive training rolled out across relevant sections.

5 With support from a commercial partner, we undertook a data mapping exercise. This required us to interview representatives from across the business to understand the nature of their role, the personal data processed in their area and the systems in place to manage this material. This provided a comprehensive GMC-wide view of our records and our use of personal data. We intend to maintain the data map on an ongoing basis. This will be of value to our information security colleagues as well as providing a resource for our internal auditors.

DPO Post-GDPR Activities and Actions

Awareness

6 We worked closely with colleagues in internal communications to develop tailored messaging in relation to the GDPR. We developed a suite of intranet pages to guide colleagues when considering a range of data protection issues. We used some new channels as well. We produced a blog article to describe our GDPR implementation.

We also developed a desk drop to coincide with go-live. We intend to develop some new internal communications items in the coming months.

7 We produced new e-learning materials for use by both staff and associates. This has been largely well received; however, we recognise that the material could be shorter. We will work with learning and development colleagues to review the training content. We are exploring the possibility of shortening the training course, in particular for those who have successfully completed the initial training course. This is based on feedback from some of our associates. Take up of the e-learning package has been high, not least because this is a mandatory piece of training.

Subject Access Requests and Information Rights

8 The GMC has typically received a high volume of subject access requests (SARs). These largely derive from our fitness to practise function where doctors and complainants request copies of their personal data. The GDPR posed some new challenges. The £10 fee which we could levy under the previous legislation was removed. We have seen a rapid increase in the number of requests we receive, partly due to the fee's removal. For the six-month period June to December 2017 we received 207 SARs compared with 267 requests over the same period in 2018. This marks a 26% increase.

9 The GDPR also reduced our statutory response time for SARs from 40 calendar days to one calendar month. It has proved challenging to manage both the increased volumes and the reduced compliance period. Nonetheless, members of the Information Access Team have managed to successfully meet their SLA since we went live with the new regime.

10 It is also notable that the GMC successfully challenged a subject access issue at the Court of Appeal in June 2018, DB v GMC [2018] EWCA Civ 1497. This is an important test case. It relates to a complainant who wanted to access a Fitness to Practise expert report regarding his treatment. The doctor in this case had refused consent for the complainant to access this material on the basis that the complainant may use it in the context of a medical negligence claim. The Court of Appeal held that this should not be viewed as an automatic barrier to disclosure as had been stated by the judge in the lower court. In practice, this has provided us and the rest of the UK with helpful clarification and demonstrates the GMC's commitment to transparency.

11 The GDPR also introduced an extended range of data subject rights including the right to rectification and the right to "be forgotten". We have received a handful of information rights requests (IRRs), most of which have been relatively straight forward. We have been asked by Fitness to Practise complainants to append their Siebel records with additional information where they feel information is incomplete. We have also dealt with requests to remove information from the public version of

the medical register. For example, a doctor asked us to remove her designated body information from her List of Registered Medical Practitioners record because she had been exposed to stalking in the past. Colleagues in Registration and Revalidation supported this request and we were able to implement a technical solution with assistance from IS colleagues.

Personal Data breaches

12 The GDPR introduced a high-profile range of duties in respect of information security breaches, including a statutory reporting regime and a Europe-wide civil penalty structure, with a much publicised maximum fine of €20m. The GMC has a highly developed information security management regime which has been in place since 2006. We are certified to the international information security standard ISO-27001. A copy of our most recent Information Security Management System report is attached at Annex A. In 2018 we experienced 155 disclosure incidents which represent a 34% increase on 2017. Root cause analysis continues to be performed and a range of activities have been undertaken to help reduce such incidents.

13 The GDPR provides a threshold at which we should consider contacting the Information Commissioner's office to notify them of a significant breach. We have not experienced any breaches which meet this threshold since we went live in May 2018.

Data Protection Impact Assessments

14 The GMC introduced a new statutory risk management tool in 2018, the Data Protection Impact Assessment (DPIA). This provides a means of analysing potential data protection risks up front. For example, project managers use DPIAs to support their risk analysis when projects require the processing of personal data.

15 Since May 2018 we have undertaken 12 formal DPIAs. For example, we undertook a review of the Contact Centre's "webchat" project. This will allow members of the public and doctors to interact with contact centre staff using a web interface. We considered the storage of these conversations, particularly where sensitive personal data is provided.

Future Plans and Policy Development

16 During the course of this year we will be closely monitoring the development of the EU's e-privacy regulation. The scope of the e-Privacy Regulation will apply to any organisation that provides any form of online communication service, uses online tracking technologies, or engages in electronic direct marketing. While the GMC does not direct market on a large scale, we need to make sure that our activities are compliant. This regulation will eventually replace the Privacy and Electronic Communications Directive, 2002.

17 The e-privacy regulation was originally to be implemented in parallel with the GDPR. For various reasons that hasn't happened and the European Commission have not provided a clear implementation date as yet.

18 We will also continue to monitor Brexit developments. The UK will no longer be subject to the GDPR outside the EU, however, the UK government has committed to full alignment with the GDPR. We have undertaken analysis of potential risks arising from Brexit in relation to our processing of personal data and we do not foresee any immediate challenges.