

Responsible Officer and Appraisal Networks Information Sheet 16a

Responsible officer function and GDPR

(v1.1, June 2018)

All organisations holding personal information need to meet the new General Data Protection Regulations (GDPR) which came into force on 25 May 2018.

It may help to bear some important principles in mind in relation to the GDPR and the responsible officer functions:

- Broadly speaking, the GDPR is intended to bring parts of the commercial sector into line in terms of their use of their customers' data for purposes far beyond what the customer thinks they have consented for.
- By comparison the data held by designated bodies about their doctors is for managing professional standards in a work context. There are undoubted responsibilities in terms of security and confidentiality of information held, but these are not new. In other areas GDPR is perhaps of less impact in the context of the responsible officer's duties. For example there is minimal scope for the passing of data to commercial third parties.

There is scope for a responsible officer to inform some third parties of data, for example to the GMC when a doctor is being referred for Fitness to Practise procedures. However, this is relatively uncommon, and often does not require consent, being governed by statutory regulations (though it is good practice to keep the doctor informed).

Designated bodies should already have written policies and protocols (sometimes called Fair Processing Notices) about the handling, storage and disposal of information relating to doctors on their list, including appraisal information, information about the doctor's practice, information relating to concerns about practice and identity checks. Whilst it may be appropriate to refresh these to refer to the new legislation there should not be a need for wholesale change to a designated body's existing approach. The statutory basis of the responsible officer functions means that the GDPR should not change the fundamental approach to data sharing.

GDPR does not necessitate a fresh communication with all individuals on existing databases. However, going forward, data controllers need to provide privacy information available to all new data subjects including arrangements around the retention and deletion of information. These policies must define arrangements around the retention and deletion of information about doctors that balance statutory requirements towards patient safety with the rights of the individual under GDPR.

GDPR Regulations:

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

Information Commissioner's Office guidance on GDPR:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

Information flows to support medical governance and responsible officer statutory

function: <https://www.england.nhs.uk/medical-revalidation/ro/info-flows/> (See Toolkit 2 for an illustrative appraisal documentation access statement).

This information sheet is relevant to all designated bodies in England.

These information sheets are written on an ad hoc basis, on issues of relevance to responsible officers and their teams, medical appraisers and doctors.