

Agenda item:	8
Report title:	GDPR and consent
Report by:	Anna Rowland , Assistant Director, Fitness to Practise, Anna.Rowland@gmc-uk.org , 020 7189 5077 Andrew Ledgard , Head of Information Policy, andrew.ledgard@gmc-uk.org , 020 7189 5418
Action:	To consider

Executive summary

The Executive Board is asked to approve our post-GDPR approach to processing personal data. We will no longer be permitted to seek consent from data subjects in the vast majority of cases, rather, we will process personal data without consent where this is *'in the exercise of official authority'*.

Recommendations

- a** The Executive Board is asked to approve "Approach Two" – a wholesale move away from consent from data subjects – as our preferred processing model when exercising our "public task", ie in the exercise of official authority.
- b** The Executive Board is asked to note the work being undertaken by Standards colleagues to update their confidentiality guidance for the profession, and plans to update the Executive Board in more detail in March.

Background

- 1** The GMC is subject to the General Data Protection Regulation (GDPR). The regulation comes into force on 25 May 2018. As now, in order to process personal data, we need to demonstrate we have an acceptable “processing condition”. Traditionally under the Data Protection Act 1998, the GMC has largely operated a consent model when handling personal data and we have used consent as our main processing condition. However, the regulation explicitly prohibits public authorities from using consent as a processing condition when exercising its statutory functions. In essence, any processing we perform under the Medical Act should use our “public task” as our processing condition. We should no longer seek consent under these circumstances.
- 2** On 27 November 2017, we brought a paper to SMT to discuss the issues raised by this change in the law (attached at Annex A). In broad terms, we felt that this would have a sizeable impact on our fitness to practise (FtP) activities given that they routinely involve the sharing of personal data for which we have traditionally sought consent. We recognised that the rest of the business would also be impacted, albeit on a relatively small scale.
- 3** Senior colleagues agreed that we should continue our impact analysis across the organisation and seek additional legal advice where necessary. SMT endorsed our proposal to undertake the necessary work to prepare for implementation of Approach Two – a wholesale move away from consent.
- 4** This paper confirms our findings and highlights the need to operate a hybrid model on a limited basis. We seek approval to continue with our work and fully implement Approach Two ahead of GPDR go-live in May 2018.

Discussion

- 5** Approach Two requires us to move away from seeking consent wherever possible, where an alternative statutory purpose exists. Under the new model we will inform data subjects about the potential use of their personal data and give them an opportunity to provide their views on our proposed usage. We make clear that our statutory duties require us to proceed in a particular manner, for example, in an investigatory context, and the data subject should be aware of the implications for the use of their personal data. For example, if a complainant raises a concern that amounts to an allegation that a doctor’s fitness to practise is impaired, they should understand we have a statutory duty to investigate and this may require us to process their personal data.
- 6** Our analysis further confirmed that the vast majority of consent collection takes place in our Fitness to Practise context. In order to implement Approach Two we will need to update a large volume of template fitness to practise letters, moving away from the language of consent. This is labour intensive, however we believe that the impact on our core IS systems will be minimal. We will not require a great deal of system development time. The transition is largely a manual exercise.

- 7** Discussions with colleagues in Registration and Revalidation indicated that consent is far less of an issue for them. There are rare occasions where we may seek consent, but this is on a small scale and their GDPR preparatory work is minimal. Approach Two works well in their context. Similarly, colleagues in Education and Standards have indicated that their work does not involve the sharing of personal data that requires consent and therefore no work is required.
- 8** From a governance perspective, our consent work forms part of the wider GDPR programme and is progressed by means of a programme board work stream that is overseen by the GDPR programme board. The programme board recognises the need to undertake communications with external stakeholders about this work. This has been highlighted with the programme communications lead and a draft plan is awaited. A training plan has been developed which will ensure staff are aware of our new approach.

Alternative Approaches in Exceptional Circumstances

- 9** Our analysis identified a small number of areas where Approach Two would be inappropriate. There are some activities where we process personal data outside of our statutory remit. For example, Human Resources colleagues may wish to share employee personal data with our occupational health partners. This activity is potentially sensitive and would not be regarded as a “public task” for GDPR purposes. Under these circumstances, the GDPR permits us to continue to seek consent from such data subjects.
- 10** Similarly, in the very specific context of Fitness to Practise Health Assessors seeking medical reports from a doctor’s healthcare provider, Senior Counsel has advised that we should seek consent to manage our compliance with our duty of confidence. It should be noted that this is **not** consent for GDPR purposes but is solely a means of managing a potential breach of confidence. This is analogous with our “Approach Three”. We have deliberately avoided using this hybrid model too widely, given the potentially confusing messaging - we’re not asking for GDPR consent, but we are asking for consent in respect of confidentiality. Approach Two works under most circumstances and doesn’t require wider adoption of this hybrid approach.

Our guidance to the profession

- 11** Our confidentiality guidance for doctors is primarily concerned with doctors’ individual ethical and legal duties of confidentiality as established in practice and the common law. We aim for the guidance to be consistent with data protection law but it is not guidance on the law. This will not change with GDPR.
- 12** Colleagues in the Standards team have analysed the changes that need to be made to the guidance so that it is consistent with the GDPR, and have tested proposals with senior counsel. The changes will be relatively minor and the redrafted guidance will be submitted for the Executive Board to note in March.

Conclusion

- 13** In summary, while this work is undoubtedly labour intensive, we are progressing with work to enable us to be in a GDPR compliant position by 25 May 2018. Additionally, removing consent from our FtP activities may see some secondary process improvements in the longer term. We seek approval to implement Approach Two.

8 – GDPR and consent

8 – Annex A

SMT Paper 27 November 2017

GDPR: Our operational approach to consent

At SMT's meeting on 30 October 2017, three options for our operational approach to consent under the General Data Protection Regulation (GDPR) were outlined. The first option, Approach one, has been discounted as it is not compliant with the GDPR.

The two remaining approaches are:

- **Approach two:** Move away from relying on consent altogether when exercising our core statutory functions – identify other lawful bases for processing personal data and defending breach of confidence.
- **Approach three:** Rely on other GDPR grounds for processing personal data but ask for consent in relation to the obtaining / disclosure of confidential information.

For the reasons that we explain in greater detail below, Approach two is the preferred option.

SMT is asked to:

1. Agree that we commit resources to understanding fully and investigating Approach two, with a view to adopting this approach prior to GDPR implementation (25 May 2018)
2. Confirm the appropriate governance route (Executive Board or SMT).

Current approach to consent

We do not always seek consent to process personal data, but primarily in FTP consent is sought where we need to disclose personal data (which may also include confidential information e.g. relating to health). Such disclosures are made in the course of enquiries or investigations into a doctor's fitness to practise. Currently this happens on a frequent basis.

Currently where consent is collected, this provides both a “processing condition” under data protection law and avoids any breach of the law of confidence. There is a process within FTP to decide whether to proceed with a disclosure in the absence of consent (where it has been refused or is not possible to obtain). These decisions are taken on a case by case basis by an Assistant Registrar.

Within R&R, consent is also sought but only on an occasional basis for the purpose of disclosing personal data and confidential information. This is usually the case where we need to disclose to third parties for the purpose of assisting an assessment as to whether a doctor should be admitted to the register or continue to hold a licence. Consent is not an issue for the vast majority of R&R activities.

Post-GDPR approach to consent

Tim Pitt-Payne QC provided preliminary advice on the approach we could take to consent following the introduction of the GDPR at an Information Governance (IG) clinic held on 15 June 2017 and subsequently at a conference with him on 15 November 2017. The key points were:

- a more restrictive approach to consent will apply under the GDPR – this includes the need to assess whether consent is freely given, it must be as easy to withdraw consent as it is to give it and data subjects will have additional rights of erasure and portability;
- Recital 43 to the GDPR states that where there is a clear imbalance between the controller and the data subject (giving the particular example of a public authority controller) it will be difficult for consent to be freely given;
- the ICO draft guidance on consent includes numerous statements regarding the difficulty for public authorities in relying on consent given the ‘power imbalance’ and suggests they should rely instead on other processing conditions;
- there is an imbalance in power between the GMC and data subjects, so it is very difficult to say consent is freely given - we should therefore rely on other GDPR processing conditions to justify our processing of personal data, and not consent;
- disclosing confidential information involves a potential breach of confidence but the requirements for consent are not as strict as the GDPR consent requirements. The potential choices here are to:
 - a seek to use our statutory functions to override a breach of the duty of confidence so we wouldn’t need to obtain consent; or
 - b ask for consent to disclose confidential information.

Counsel suggested that we would need to further analyse potential choice (a). We have started work in this area, and this forms the basis of our preferred option, approach two.

Approach two

- Compliant with GDPR, ICO's (draft) guidance and Counsel's preliminary advice. Counsel will provide formal written advice in due course.
- Starting point is that we rely on other legal bases to justify our use/disclosure of personal data and confidential information (i.e. our statutory functions and powers under the Medical Act or where processing is in the public interest).
- To balance possible reputational risk we will tell individuals how we intend to use information about them. In the areas where we currently seek consent (principally in FtP and the occasional area in R&R), we will provide an opportunity for the individual to make representations regarding the use of their information. Where representations are received, we would take these into account to inform our decision whether disclosure of confidential information is justified in the particular circumstances. This is consistent with Counsel's advice and will assist us to manage our obligations under the Human Rights Act.
- This approach is the most straightforward to communicate to individuals and least likely to lead to confusion.

Risks: This is the biggest change in position from the current process and may appear to individuals that they have lost control over their information. However, this can be managed by allowing the opportunity to provide representations.

In addition, individuals will not be entitled to rights associated with consent such as the "right to be forgotten" and data portability etc.

Currently, the GMC's approach to consent is aligned with our guidance to the profession and this would change. However, a divergence in approach is justifiable based on our different functions and different (and changing) legal powers.

Operational impact: An early analysis of the operational impact suggests this would require some Siebel changes to remove consent processes, there may be a decrease in operational effort as a result of removing the consent stages, FTP investigation times may reduce.

Since the last SMT, we have undertaken further analysis in relation to Approach two:

- Legal fully reviewed the instances where we currently seek consent in FTP and R&R and highlighted the areas where we need to obtain further advice from Tim Pitt-Payne QC; and
- FTP Policy prepared a short discussion paper to aid consideration of the dialogue we will need to have with individuals in the future if we are not seeking consent. These documents were considered by the FTP SMT on 8 November 2017.

At an FTP SMT meeting on 8 November it was agreed that Approach two would be their preferred option and suggested the following:

- The tone of voice in letters/forms will be critical
- We should ask the individual whose data we propose to use to confirm that they understand that we have powers to disclose as well as asking if they want to make any representations (e.g. please tick this box to confirm that you understand we have this power...)
- A deadline of 14 days was agreed as a sensible period to allow for representations and it was also agreed that we would not chase after that period
- The approach will need to be communicated with Trusts and it was agreed that Comms/ELS/RLS could assist

Approach three

- Compliant with GDPR and ICO's (draft) guidance.
- This approach would be difficult to communicate clearly. Under the GDPR we have to communicate clearly with data subjects so they understand how we use their personal data. If we do not seek GDPR consent but ask for consent to avoid a breach of confidence, this is potentially very confusing.
- If consent is refused, we would still need to consider whether there is an overriding statutory function or public interest in proceeding.

Risks: Individuals will not understand the distinction between us not requiring consent for data protection purposes, when they are still being asked for consent in relation to the duty of confidence. Currently, we do not make the distinction between consent for different legal regimes. They may be confused about what rights are open to them under each legal regime. This could lead to increased dialogue/complaints.

Operational impact: Early analysis suggests this would require Siebel changes and operational effort will be maintained as duty of confidence consent will need to be addressed in the same level of cases. Any confusion around a dual approach to consent could result in additional resource being required to respond to questions and address duty of confidentiality consent and possible complaints. Investigatory steps relating to redaction could also be complicated by a hybrid approach to consent.

Legal advice

Legal have instructed Tim Pitt-Payne QC to provide formal written advice regarding approach two which should be provided by the end of November. At a telephone conference with Counsel on 17 November, he confirmed that the internal legal analysis already undertaken evidences a robust basis for relying on statutory authority or

overriding public interest rather than consent, and that there is nothing to prevent us from adopting the preferred approach.

Counsel also confirmed that where we will be relying on another legal basis post GDPR, we will not need to retrospectively contact individuals regarding consent requested or received prior to GDPR implementation.

Next steps

A series of workshops are planned to identify the operational impact of Approach two, and to confirm the system change requirements to allow the Siebel team to build these into the dedicated GDPR Siebel release in May 2018. We will bring our findings to either SMT or the Executive Board for final approval. We would welcome confirmation of Director's preferred governance route.

Decisions for SMT

1. Agree that we commit resources to understanding fully and investigating Approach two, with a view to adopting this approach prior to GDPR implementation (25 May 2018)
2. Confirm the appropriate governance route (Executive Board or SMT).

Annex

- [ICO Draft GDPR Consent Guidance](#)