HAT Technical

MEMO 10/18

To: All firms
From: Simon Kettlewell
Date: 14 May 2018

GDPR AMENDMENTS TO ENGAGEMENT TERMS

All firms should be aware that the new data protection legislation, the General Data Protection Regulation ("GDPR"), becomes effective on 25 May 2018.

All engagement letters issued prior to 25 May 2018 refer to the Data Protection Act 1998 and therefore need to be updated to reflect the relevant legislation that comes into force after that date. The simplest mechanism for doing this is to issue an amendment to the existing letter. Assuming firms have followed the cover letter/ service schedule/ terms of business format for their engagement letters, as encouraged in our manuals, this will be achieved by issuing an amending covering letter which repeals the existing data protection text from the terms of business and adds in the GDPR-compliant text. Where firms have not followed this approach, it should still be possible to 'patch' existing letters rather than re-issuing them in full; however, wording will need to be amended as appropriate.

For existing clients it is recommended that letters are updated from 25 May onwards. If firms wish to update letters prior to this, the wording we have provided should make it clear that the new terms only apply from 25 May onwards. The ICAEW/ ACCA/ ICAS normally recommend obtaining the client's explicit approval for amended terms and we have therefore followed this approach in our suggested wording. For all new engagement letters issued after 25 May 2018, an updated covering letter and updated terms of business will need to be issued alongside the usual service schedules.

HAT have drafted an 'amendment of terms' letter for those clients where existing engagement letters are in place, as well as updated terms of business to be appended to new engagement letters issued post 25 May 2018. These documents can be found in the "Proforma documents - May 2018" folder in the members area of www.hatgroup.co.uk.

Our updated guidance is designed to be suitable for a typical firm of general practice accountants and does not cover every eventuality. If you have concerns about the wording you should refer to the more detailed guidance noted below which is available from the ICAEW / ACCA / ICAS and if necessary obtain legal advice. In particular, our updated terms only relate to the situation where the practice is a data controller and a GDPR-compliant privacy notice is displayed on the practice's website. Further detail on these caveats is set out below.

Is my firm a data controller or a data processor?

Determining whether you are a data controller or data processor in respect of your client is important as it dictates the contents of your terms of business in respect of GDPR. The Information Commissioner's Office (ICO) believe that accountants acting on behalf of clients are always data controllers rather than data processors. Per paragraph 27 of the ICO's "*Data controllers and data processors: what the difference is and what the governance implications are*" (available here: https://bit.ly/1zjRqM3);

"the client will not have sole data controller responsibility even though they initiated the work by asking for advice or commissioning a report. Responsibility also lies with the professional service provider itself because it determines what information to obtain and process in order to do the work and because it is answerable itself for the content."

Paragraph 44 goes on to state:

"When acting for his client, the accountant is a data controller in relation to the personal data in the accounts. This is because accountants and similar providers of professional services work under a range of professional obligations which oblige them to take responsibility for the personal data they process. For example if the accountant detects malpractice whilst doing the firm's accounts he may, depending on its nature, be required under his monitoring obligations to report the malpractice to the police or other authorities. In doing so an accountant would not be acting on the client's instructions but in accordance with its own professional obligations and therefore as a data controller in his own right."

HAT are aware that this is an area of some contention as previously it has been suggested that firms providing services such as payroll would only be a data processor when undertaking that service. The ICAEW are seeking to obtain definitive guidance from the ICO on the status of providing services such as outsourced payroll provision. In the meantime, our pro-forma wording is drafted assuming that firms act as data controllers for all clients.

Privacy notices

The ICAEW, ACCA and ICAS have recently released their template privacy policy wording. It is expected that firms will make use of the relevant template from their regulator and publish their privacy statements on their website. **PLEASE NOTE**: It is the responsibility of each practice to ensure that the engagement terms are consistent with the privacy policy. Privacy policy statements must be tailored to suit the individual firm's circumstances. If a firm has any doubts over their obligations here, they should seek advice from their regulator and/ or lawyer.

Other resources

There are a number of useful other documents published by the ICAEW, ACCA and ICAS which firms should review as appropriate.

- ICAEW firms: https://bit.ly/2rFVfAx
- ACCA firms: https://bit.ly/2Khy0U7 and https://bit.ly/2IgOjQq
- ICAS firms: https://bit.ly/2wEkeJ7

We are aware that a number of firms have already taken significant steps to becoming compliant with GDPR, whilst other firms have not made much progress. It is worth remembering the following piece of guidance from the ICAEW: "*The ICO is not expecting every organisation to have all policies and procedures in place on 25 May 2018 but it will expect every organisation to have made a start and to have a plan on how it will be GDPR ready and when.*"

It is not possible for HAT to provide prescriptive procedures on how to comply with GDPR as this will depend on the size of your firm, how you operate and the complexity of your services and systems. However, we are covering GDPR in detail in our Q2 Update, which we are also running in the HAT office on 7 June and 5 July. To make a booking please email maggie@hatgroup.co.uk.

We are always pleased to receive feedback on our manuals. If you have any comments then please email simon@hatgroup.co.uk