22 City Road
Finsbury Square
London EC1Y 2AJ

Tel: +44 (0) 20 7448 7100
Email: info@pimfa.co.uk
Website: www.pimfa.co.uk

UK Parliament
Public Bill Committee
scrutiny@parliament.uk

13 March 2018

Dear Sirs

DATA PROTECTION BILL – PROCESSING OF HEALTH DATA BY PRIVATE FINANCIAL ADVISERS, PLANNERS, AND INVESTMENT MANAGERS

The PIMFA would like to draw attention to an issue with regard to the Data Protection Bill that relates materially to the work of PIMFA member firms.

The issue pertains to the processing of special category data under the General Data Protection Regulation (GDPR) which will come into force on 25 May 2018. The Data Protection Bill, currently being discussed in Parliament, will give effect to the GDPR in the UK and when completed will replace the current Data Protection Act.

Special category data is defined by Article 9(1) of GDPR as *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.

This Article represents a prohibition on processing special category data unless (i) processing meets one of the conditions for processing in Article 9(2), or (ii) a specific derogation is introduced under Article 9(4).

Article 10 GDPR is a restriction on the processing of personal data relating to criminal convictions and offences.

Clause 10 of the Data Protection Bill - *Special categories of personal data and criminal convictions etc data* - specifies some of the conditions of processing permitted under Article 9(2) of GDPR (special category data) and under Article 10 (criminal convictions and offences data). The details of the conditions are included in Schedule 1 of the Data Protection Bill.

[1]The Personal Investment Management and Financial Advice Association (PIMFA) is the UK's leading trade association for firms that provide investment management and financial advice to everyone from individuals and families to charities, pension funds, trusts and companies.

PIMFA was created in June 2017 as the outcome of the merger between the Association of Professional Financial Advisers (APFA) and the Wealth Management Association (WMA) and represents both full and associate member firms.

PIMFA's mission is to create an optimal operating environment so that our member firms can focus on delivering the best service to their clients, providing responsible stewardship for their long-term savings and investments. We also lead the debate on policy and regulatory recommendations to ensure that the UK remains a global centre of excellence in the investment management and financial advice arena.

Our concerns relate to the processing of special category data in the context of information about people's health.

Of interest to us are Article 9(2)(g) of GDPR, and Clause 10(1)(b) and Schedule 1 of the Data Protection Bill.

Schedule 1, Part 2, para 15 of the Data Protection Bill contains a condition allowing firms to process health data in certain circumstances if this is necessary for the purpose of carrying out insurance business.

The derogation as drafted is specific to insurers and does not apply to private financial advisers, planners and investment managers, as they are not carrying out insurance business.

Private financial advisers, planners and investment managers necessarily receive information regarding client's health in order to provide their service and act in the best interest of their clients. Acting in the best interest of the client is a regulatory obligation that firms need to comply with under MiFID II (and consequent FCA rules).

For example, a health deterioration in any client but particularly in an elderly client will be a trigger to reassess their investment objectives and attitude to risk e.g. a client of this type may need to raise funds to help fund care costs, they may also need to lower risk to protect their investments from market volatility and/or may move from a capital bias portfolio (i.e., mainly equities) to an income bias portfolio (i.e. mainly fixed income) to help maintain the cost of care into the future. If firms are not made aware of such information they are unable to act upon it and to act in the best interest of the client.

When carrying out KYC, firms ask the client to consider any circumstances which impacts or may impact their investment objective and attitude to risk, which may entail the disclosure of health information. The client or a representative of the client may subsequently contact the firm to update the firm of a health situation. The clients of private financial advisers, planners and investment managers have a close, ongoing relationship with their Investment Manager or Financial Adviser/Planner and therefore over the years a wealth of information may be shared, from the location of family holidays to notifying the firm of a negative medical diagnosis.

Under GDPR, the only lawful grounds available to private financial services firms processing customers' health data is 'explicit consent'.

This represents an issue as

- The introduction of Article 7(4) GDPR means that, technically, 'explicit consent' is not "freely given" in these instances, as it is needed for the performance of a contract – withdrawal of consent by the customer would thus result in termination of the business relationship. This is confirmed by Recital 43 GDPR, whereby *consent is not presumed to be freely given […] if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*, as well as by Article 29 Working Party's comments on page 9 of their draft Guidelines on Consent: *the necessity for performance of contract is not a legal basis for processing special categories of data*; and

- In the case of vulnerable customers who for any reason are mentally incapacitated because of a health condition, it is debatable whether 'explicit consent' can be obtained at all, so the firm could not perform its duties or act in the best interests of their client.

  On this point, we note the condition in Article 9(2)(c) of GDPR - *processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent*. This could potentially be appropriate for the vulnerable customer scenario. However, it is not clear how the provision will apply in the UK as there is no reference to it in Clause 9 of the Data Protection Bill. Moreover, the wording "vital interests" is not defined, and there is no assurance that protecting a person's finances be considered within scope.

We draw attention to the "substantial public interest" lawful ground under Article 9(2)(g) of GDPR. In our view, processing of customers' health data by private financial planners, advisers and investment managers, for the purpose of performing their duty to act in the best interest of the client, could be considered as being carried out to fulfil a substantial public interest.

Our view is based on the fact that these activities are about much more that investing an individual's savings. Private financial advisers, planners, and investment managers have to assess an individual wholly, covering such aspects as his or her financial situation, age and health, family ties, needs, hopes and objectives, and make a proposal together with the individual concerned to meet personal needs and objectives in a long-term sustainable way.

However, Article 9(2)(g) leaves the definition of "substantial public interest" to each Member State, which means that there is no guarantee that a derogation will be granted.

As matters currently stand, unless this situation is clarified, the risk is that a great part of retail financial services firms will be forced to process their customers' health data on non-appropriate grounds, or cease business activities.

Here are some possible approaches that could resolve the inconsistencies.

1. General derogation

A way to resolve the issue could be a general derogation, permitting firms carrying out private financial advice, planning or investment business to process customers' health data on "substantial public interest" grounds where the processing is for the provision of their services and the performance of their duty to act in the best interest of the client.

Here is a possible draft general derogation for your consideration:

In Schedule 1, Part 2, add at the end

> *Personal financial advice, planning and investment*
>
> *24(1) This condition is met if the processing*
>
> > *(a) is necessary for the purposes of carrying out personal financial advice, planning or investment business so that the duty to act in the best interests of the customer can be met, and*

(b) is of data relating to the health of customers of the personal financial advice, planning, or investment businesses.

(2) Personal financial advice, planning and investment business is the provision of regulated activities to individuals, subject to suitability obligations and the requirement to be in line with the individual's objectives and needs.

(3) Regulated activities are those included in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, and any amendments thereto.

(4) For the purposes of this paragraph 22, a customer is a client of a personal financial advice, planning or investment management business who is a natural person.

2. Interpreting Article 9(2)(a) and 9(2)(c) of GDPR

An alternative approach to a general derogation could be to interpret the relevant Article 9 categories in a way that is compatible with the needs of clients of private financial services firms.

This specifically would entail:

- Interpreting "explicit consent" under Article 9(2)(a) as "freely given" when a data subject consents to the processing of health data by a private investment manager or financial planner or adviser, so that the business can provide their services and perform their duty to act in the best interest of the client;

- Interpreting "vital interests" under Article 9(2)(c) to include a person's interest to the protection of their finances. This would allow private investment managers and financial planners and advisers to process a customer's health data when the customer is not in the condition to provide explicit consent, enabling them to provide their services and perform their duty to act in the best interest of the client.

  An example of the benefit of such interpretation could be the case of a customer suffering a stroke and not being able to look after themselves. Interpreting the customer's interest to the protection of their finances as a "vital interest" would allow the firm to receive and process this information and to make the right investment choices to ensure the customer can pay for adequate care.

3. Regulatory mandate

If Parliament was against the inclusion of a derogation or interpretation in the Data Protection Bill, an effective result could also be obtained by way of a principle-based exception with mandate to the Information Commissioner's Office – together with the Financial Conduct Authority when the matter concerns financial institutions – to interpret Article 9 in a way which is compatible with the UK's regulatory landscape and to produce rules and guidance that are considered reasonable and proportionate to safeguard both the public and the business community.

This approach would have the advantage of "future-proofing" the legislative text, leaving space to the regulator to fine-tune the application of the rules to fit the needs of modern society.

PIMFA – 13 March 2018