WEALTH
MANAGEMENT
ASSOCIATION

10 May 2017

Data Protection Team
Department for Culture, Media & Sport
4 th Floor
100 Parliament Street
London SW1A 2BQ
GDPRCallforViews@culture.gov.uk

Dear Data Protection Team

WMA's[1] response to DCMS's Call for views on the General Data Protection Regulation derogations

Our detailed response to the questions in the Consultation are set out in the appendix accompanying this letter.

If you have any further queries please do get in touch.

Yours faithfully

[1]The Wealth Management Association (WMA) is a trade association that represents 180 wealth management firms (full members) and associate members who provide professional services to our full member firms.
WMA members firms look after over £825 billion of wealth for over 2.2 million retail investors.
WMA full members deal in stocks, shares and other financial instruments for individuals, trusts and charities through a range of services spanning execution only, advisory and discretionary fund management.
The WMA exists to support its members and their clients through education and engagement, advocacy and influence, research and analysis and by playing an active role as a facilitator and thought leader.
WMA firms operate across more than 600 sites, employing over 27 000 staff. These firms also run over 5.5 million client portfolios and carry out over 20 million trades a year.

Wealth Management Association (WMA)
Company limited by guarantee
Registered in England and Wales No. 2991400
VAT Registration No. 675 1363 26
EU Transparency Register Member: 855507915268-60

DCMS Consultation on Data Protection Derogations – WMA Response

Theme 1 – Supervisory Authority

Article 51 – Supervisory Authority

It is our understanding that the ICO will be the supervisory authority for data protection in the UK.

It would be helpful to have clarifications of how the ICO and the FCA will interact when it comes to compliance with data protection requirements by FCA authorised persons, given that there are overlaps between GDPR and the MLR and MiFID. Another source of potential conflict is the FCA's Senior Managers Regime (SMR), especially around whether data ownership or responsibilities could be specific as part of SMR role specifications.

Article 58 – Powers

Article 58(4) refers to "safeguards" to be put in place for the exercise of the supervisory authority's powers. We would like to stress the importance of proportionality as an overarching principle of the exercise of power.

Theme 2 – Sanctions

Article 84 – Penalties

In our view, the current administrative penalties are sufficient.
The GDPR purports to impose fines of up to 4% on global turnover; however, WMA members are deeply concerned about the lack of clarity as to what global turnover means and if/when it would include other group companies' turnover when calculating the percentage fine. Currently, recital 150 of the GDPR refers to penalties being imposed on an "undertaking", and refers to Articles 101 and 102 TFEU, however the meaning of undertakings is not defined in those TFEU articles. Owing to the potentially significant effect this would have, firms would greatly benefit from clarifications about when a fine would be imposed using a percentage of the group's turnover, rather than against the relevant entity which is found to have breached the GDPR.

Theme 3 – Demonstrating compliance

Article 40 – Codes of Conduct

WMA member firms are concerned about the potential fragmentation that could be caused by different Codes of Conduct being adopted by different sectors and at different times within the financial services space.

It is not uncommon for a firm to perform more than one business activity, therefore firms would need to know what to do if they are required to comply with different Codes of Conduct for different business areas in the event of an inconsistency between such Codes.

WMA member firms would like DCMS to consider whether some form of guidance for the financial services sector as a whole, coming for example from the ICO and the FCA and aimed at reducing the risk of inconsistencies between single sector Codes of Conduct, would be useful.

Article 42 – Certification and Article 43 – Certification bodies

We support the certification system as it creates business and consumer confidence, on the one side by making proof of compliance easier and on the other side by providing customers with an easily identifiable way of assessing the business they wish to enter into a relationship with.

In terms of certification process and bodies, WMA member firms suggest using an existing standard such as ISO27001 with some specific guidance around controls that can be included in the Code of Conduct. Certification could then be done by the BSi or a BSi accredited organisation.

There is a British Standard for data protection compliance with the Data Protection Act 1998, that is 10012:2009, but to our knowledge it is not widely used and there are no plans to update it. If it was agreed that this is the standard to be used, therefore, it would need to be updated and its use encouraged.

Theme 4 – Data Protection Officer

Article 37 – Designation of Data Protection Officer

In our view, there is no need for additional legislation and we welcome the flexible approach of the GDPR which allows each firm to exercise its judgment as to the appointment of a Data Protection Officer.

On the other hand, rather than black-letter law, we would welcome guidance helping firms understand whether they would need a Data Protection Officer, for example by providing clarifications on how the regulator would interpret:

- *"large scale processing", also in relation to the "systematic monitoring of data subjects" and "processing of special category data"*
- *the processing of special category data when the processing of these data is non-core but the business relies on it – for example when health data is processed by a wealth manager in order to provide comprehensive wealth planning services*

We acknowledge that Art. 29 WP has produced some guidance on the topic. However, WMA member firms feel that the existing guidance is still not sufficient to establish unambiguously who does or doesn't need a Data Protection Officer. This is a costly and important position and firms need to have more certainty about when they need one.

In addition, can the DCMS provide guidance in relation to whether or not an in-house lawyer can also be a Data Protection Officer (i.e. job share at the same company)?

It has been suggested that the Solicitors Regulation Authority's Codes of Conduct on the lawyer's requirements to act in the best interest of the company means that an in-house lawyers would not have the required independence to act as the Data Protection Officer. However, it appears to us that one of the main categories of people who will have the

likely required experience in data protection are lawyers. It also appears that some organisations who either do not require a full time Data Protection Officer or opt to have a Data Protection Officer would sensibly appoint an in-house lawyer to the position.

Finally, will Data Protection Officer be recognised by the FCA as a control function/Senior Management Function?

Article 38 – Position of the data protection officer

There are currently no rules requiring Data Protection Officers to be bound by confidentiality and secrecy with regard to the performance of their duties, which means that this is left for each firm to regulate in their own contracts of employment with the relevant individuals.

Given how diverse the UK business landscape is, having a blanket secrecy legal or regulatory requirement may create implementation difficulties. Therefore, we suggest that this issue is dealt with by means of a recommendation within the Code of Conduct applicable to each business area.

Theme 6 – Third country transfers

Article 49 – Derogations for specific situations

WMA member firms effect their third country transfer under Article 46 therefore they do not seek additional derogations.

However, WMA member firms believe that they would benefit from more guidance on when they can use explicit consent under Article 49, in particular whether this is limited to specified and limited transfers or whether it would be sufficient for systemic data transfers.

This is particularly relevant where the regulated firm is part of a group and therefore does take on systemic data transfers between different countries.

Theme 7 – Sensitive personal data and exceptions

Article 9 – Processing of special categories of personal data

Para 4 states that "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health".

(a) Use of biometric data as one of the factors for customer identification is a technology that is being developed and implemented as part of "digital identity" projects, therefore imposing additional prescriptive limitations to the use of these data (with the customer's explicit consent as per Article 9) could have the unwanted effect of stifling innovation and indirectly adversely impacting the UK's competitiveness in the field of technology.
(b) We call for identification of "explicit consent" as self-standing lawful ground rather than as an enhanced form of Article 6 "consent".

"Consent" is defined by Article 4(11) as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement

or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

The processing of health data (which is a special category data under Article 9) is necessary for the proper performance of financial planning services. This makes the processing of special category data a condition of the service, which in turn means that the customer would have no "free" consent: the firm would not be able to provide the service without taking into account the client's personal health situation, therefore consent would not be freely given.

The ICO's recently drafted Consent Guidance advises against using consent if this is a condition of service.

Therefore, if we accept that "consent" and "explicit consent" share the same general requirements, this would put firms at risk of breaching GDPR whichever course of action they choose to take – other than ceasing financial planning activities altogether, which we believe is not an intended consequence of GDPR.
This issue was already raised with the ICO in the context of their draft Consent Guidance.

Theme 9 – Rights and remedies

Article 17 – right to erasure

Article 17(3)(b) derogates to the right to erasure "for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

With regard to data retention, it is worth noting that:

- *The new SYSC 10A.1.12 R requires firms to keep the records of client instructions (including telephone recordings) for a period of five years and, where requested by the FCA, for a period of up to seven years;*
- *Regulation 39 of the new Money Laundering Regulations 2017 requires firms to retain customer records for a period of five years after the end of the business relationship.*

WMA member firms will need to comply with these prescriptive requirements.

Moreover, FCA and FOS do not recognise long-stop. What this means is that the FOS or FCA could ask at any point for a client file which is 10, 20 or even 30 years old.

This leaves firms in a difficult position as to how do they comply with the data minimisation principle which essentially requires firms to delete client data when they no longer need it (as well as the client rights around data erasure). We can see with PPI claims and endowment claims working examples of this in practice. Looking at the pension field, as we understand it, there is a statutory requirement to keep client files indefinitely.

It is unclear whether this is applied to all client files across the financial services sector until such time that the FCA recognise a long stop. Therefore, whatever the long stop is set at should be what retention period a firm sets.

This does not mean that firms can't take steps to protect client data - it may be that as part of this compromise, firms use pseudonymisation in order to 'scramble' personal data and to a) alleviate a lot of the risk of storing the personal data and b) restrict access to the data.

Another issue raised is whether a firm can ever be completely satisfied that data has been erased – there are situations whereby data erasure is either impossible or disproportionately cumbersome due to various factors such as the length of a business relationship.

It is worth noting that "erasure" is not defined. It is also worth noting that the German data protection legislation allows for the blocking of data as an appropriate alternative to erasure in specific cases including when erasure is no possible or is disproportionately cumbersome or when there is an unresolved dispute as to the correctness of the data (para. 35 BGSB).
DCMS may want to use the derogation to define erasure and to consider those situations where erasure would be excessively risky, impossible or disproportionate in order to avoid the risk of systemic non-compliance with GDPR on this matter.

In addition, and as a general comment, WMA member firms raised concerns with the processing of all those "residual data" other than client and employee data, for example:

- *Marketing data from subscription lists*
- *Data obtained from prospects who fail to become clients*
- *Function/event invite lists*
- *Details of job candidates who are not then employed by the firm for various reasons (not interviewed, not offered job, refused offer)*

These data, especially if historic and imported from legacy systems, can be problematic in that the firm may find that it doesn't know that it holds the data, or may not be able to access it or to erase it.

This can have an impact on several fronts, including data retention, erasure and grounds for processing, and represents a risk of non-compliance for firms that may be difficult to manage and potentially out of the firm's control (e.g. data stored on legacy systems of a business acquired by the firm that due to corruption cannot be accessed by the firm).

There may be scope for DCMS to consider whether, in specific circumstances, it would make sense to allow for firms to retain legacy data.

In any event, WMA member firms would greatly appreciate guidance and insight on how firms can deal with this data in an appropriate and compliant manner.

Theme 12 – Processing of data

Article 6 – Lawfulness of processing

Article 6(3) requires that the legal basis for the processing of data under Articles (6)(1)(c) – compliance of a legal obligation – and (f) – public interest – be laid down by EU or national law.

GDPR does not define "legal obligation".

"Legal obligation" could be defined as any obligation generated by law or regulation. It is pivotal that any definition of "legal obligation" includes regulator-made rules as this is where the majority of the specific rules that firms need to comply with originate.

Article 35 – Impact assessment

WMA member firms noted that the Art. 29 WP Guidance on Data Protection Impact Assessments mentions "data processed on a large scale". As already discussed in our comment under Article 37, it would be useful to have additional guidance with regard to this wording.

In particular, it would be useful to have examples of what "large scale" is, with quantitative indicators if possible.

Article 37 – Designation of the Data Protection Officer

Please see our comment under Theme 4.

Article 87 – Processing of the national identification number

It is our view that additional legislation would not be helpful as the processing of national identification number data can already be carried out efficiently on the basis of Article 6 lawful grounds.

The creation of solid certification systems in accordance with Article 42 and 43 would ensure that national identification number data is adequately protected without the need for additional prescriptive rules.

Theme 13 – Restrictions

Article 23 – Restrictions

Please see our comment under Theme 9 – Rights and Remedies, Article 17.

WMA members would also appreciate guidance on what data the ICO would expect as "machine readable" under Article 20 and in what structure this data should be. Would the ICO expect firms to agree a format between ourselves or will they provide some schema on how firms be expect to export and import data?

Other additional potential derogations under Article 23(e) could be drafted to similar effect to those already included in the new German data protection legislation.

This new German legislation contains restrictions that

- *limit information rights and data subjects' rights if giving out certain information "would involve disproportionate effort or make it unlikely to achieve the aims of the data processing"*
- *restrict purpose limitation, making it easier for firms to use data collected once for other purposes.*

Whilst we are not necessarily seeking to mirror these amendments, the GDPR is very inflexible in parts, which makes it difficult and costly for companies to comply with.

The situation is exasperated in those instances where the GDPR does not actually, in our members' view, provide the intended or practical safeguards to consumers and simply increases costs.

Examples of rules that could potentially lead to disproportionate costs for firms if applied without restrictions are Article 15 (right of access), Article 16 (right to rectification), Article 17 (right to erasure) and Article 20 (data portability).

We are looking to have proportionate, reasonable rules that do not force firms into non-compliance for impossibility (physical or financial) to satisfy requirements. With this in mind, we would urge DCMS to consider making practical exceptions, where possible, to the GDPR to allow firms to apply a common sense approach to certain situations.

Additional question – cost impact

WMA member firms believe that more guidance on how firms can implement GDPR would be a useful and effective way of reducing costs and burden to business. The danger is that firms spend a lot of money implementing the GDPR and they are then told that actually the goal posts have moved and they need to take a number of other steps in order to comply. This would cause a lot of frustration and wasted resources. Therefore, it would be helpful if the DCMS could push the relevant bodies to release a lot more detailed guidance and as soon as possible.

Having clear guidance would be helpful for everyone and especially for those smaller businesses who do not have the time and resources to employ personnel or pay for consultants in order to successfully implement GDPR with their organisation.