GDPR for advisers

January 2018

Article from Professional Adviser 24/01/18

The implementation of the GDPR has provoked concern around the data retention obligations of financial advice firms in relation to data subjects looking to exercise their rights that may require restriction of processing of their personal data or possible deletion. This has centred on the potential impact on a firm's ability to meet regulatory requirements and/or defend a legal claim should they have to delete personal data.

The question of whether a firm is required to delete personal data, or restrict its processing, is addressed in the GDPR and relates in part to the data controller's basis for processing the personal data. It will be necessary for a firm to assess each request on its facts.

At least one of six criteria must be met for a data controller to lawfully process a data subject's personal data. Importantly, a data controller must understand what condition it is relying on, since the conditions come into play in the context of how a data controller responds to a request to delete or restrict the processing of the personal data.

According to article 6 of the GDPR, processing shall be lawful only if and to the extent that at least one of the following applies:

* The data subject has given consent to the processing of their personal data for one or more specific purposes;

* Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;

* Processing is necessary for compliance with a legal obligation to which the controller is subject;

* Processing is necessary to protect the vital interests of the data subject or of another natural person;

* Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

* Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data - in particular where the data subject is a child.

The working group discussed each of the six conditions in more detail to reach a common consensus and understanding as to what lawful processing would look like from the perspective of financial advice firms.

* Consent: Whether the data subject has given consent for their personal data to be processed or not should, in theory, be very black and white. If they have consented to a firm processing their personal data, then the firm may process it.

Consent can be withdrawn at any time, however, and a firm should ensure it is as easy for a data subject to withdraw their consent as easily as it was given. Furthermore, consent should not be indefinite and firms will need to have a process by which they obtain renewed consent from data subjects - within the working group discussions, two years has been mooted as an appropriate lifecycle timeframe for consent.

* Performance of a contract: This is fairly self-explanatory. Where a firm has a contract with an individual, the firm needs to process that individual's data in order to perform services under the contract - for example, in the case of financial advisers, to provide portfolio updates.

* Legal obligation: Financial advice firms are, for example, subject to FCA record-keeping requirements. This constitutes an example of a legal obligation to which firms are subject being the basis for lawfully processing personal data.

MiFID II is another example, since advice firms will need to comply with the record-keeping requirements laid out in the directive, which involves data processing and such legal obligations will also potentially impact on other GDPR compliance aspects, such as data retention periods.

* Vital interests: This is not expected to be applicable to financial advice firms.

* Public interest: This is not expected to be applicable to financial advice firms.

* Legitimate interests: This could extent to situations such as the necessity of defending a legal claim. The firm would need to continue processing the individual's personal data in order to be able to call upon it in such circumstances.

The working group talked through a number of scenarios relating to what interaction they have had with data subjects, with a view to understanding what the data retention period would be. It was also discussed how firms would respond to a data subject exercising their right to erasure or a right to restrict processing.

In the context of financial adviser firms, the lawful conditions most likely to be relied upon are consent, delivering on a contractual commitment, meeting a legal obligation (in this case FCA regulatory requirements) or the legitimate interests of the data controller (the firm) where this did not override the rights of the data subject.

How long a firm can resist a right to erasure request and keep hold of the personal data is heavily influenced by the Financial Ombudsman's time limits on when a consumer can make a complaint - specifically: "Six years from the event the consumer is complaining about (or, if later, three years from when the consumer knew, or could reasonably have known, they had cause to complain).

"Under the rules, we have the discretion to look at complaints that fall outside these time limits in ‘exceptional circumstances'. An example of this might be if the consumer was incapacitated during the period when they could have complained."

The above time limits mean a customer of a financial advice firm could make a complaint at any point in the future. The FCA's "exceptional circumstance" criteria mean there is no fixed backstop to when a customer could complain.

It was also the view of the working group that a customer could make a complaint even if advice had not been given, let alone advice acted upon - for example, a customer has signed a customer agreement (which contains correct and appropriate privacy notice information) but no meeting with an adviser ever occurs.

The customer then makes a complaint to the Financial Ombudsman at some point in the future, that they have been negatively impacted financially as a result of the firm's representative not meeting with them and providing advice.

As a result of this scenario, the working group's view was that, once the customer had signed a customer agreement, they would look to store, if not actively process, the customer's data at least until the customer was deceased. While, to be covered by GDPR, a data subject must be living, there are still obligations relating to protecting confidential information of deceased individuals.

Cost-benefit analysis

What, though, if advice firms did delete all previously held personal data? One attendee said their firm had conducted some research into the cost of retention and processing, versus a complete deletion of all former clients, with the trail cost being the inability to defend legal claims and the subsequent settling of such complaints. They had found it did not make too much difference - the cost of settling claims did not outweigh the cost of retaining and processing old personal data no longer used by the firm.

Another attendee, however, said the retention and use of old personal data in defending legal claims had saved their firm a fortune - and potentially even kept it in business. Without the personal data, they would not have been able to defend a number of legal claims to prove they had conducted themselves appropriately, which would have voided their insurance and cost them a fortune.

There is a scenario where a lead has come into the firm but the lead has gone cold - so the individual initially expressed an interest in a product or service offered by the firm, no client agreement has been signed and no further contact has been made. This individual may still be on a mailing list, but no further interaction has taken place and certainly no further expressions of consent made in regard to receiving contact from the firm. Should such an individual's personal data be deleted or the processing of it restricted?

One working group firm said it retains leads for 18 months before deleting them. It was further discussed that a two-year retention would be acceptable. If no further expression of consent has been received, it would be best to remove this individual's personal data from your records. This will reduce the likelihood of mishaps leading to breaches.

It is strongly recommended that firms build a table that covers the various scenarios involving data subjects exercising their rights that are likely to impact their business, and establish prepared guidance as to how long they will retain personal data and how they might respond to restriction of processing or erasure requests and on what grounds.

Rob Walton is chief operating officer at Intelliflo

Lawful processing: Working group conclusions

* Given there is no clear limitation on when a firm could receive a complaint from a data subject, it is felt advice firms can legitimately reject a right to erasure request on the grounds of potentially needing to defend a legal claim. As such, firms could store personal data on a data subject until the data subject is deceased (assuming the grounds to reject a right to erasure request was also valid).

* Each firm will need to define at which point they deem the interaction with a data subject exposes the firm to a potential complaint. The working group felt this was broadly when the data subject has signed a client agreement.

* It is much more likely firms will need to support the right to restrict processing requests after rejecting a right to erasure request.

* It is important to note that restrictions on the processing of personal data are likely to be temporary, whereas deletion is permanent. Restricted personal data must be treated similarly to deleted personal data, however - subject to certain exceptions such as the need to process as part of legal claims - the only processing allowed of restricted personal data is the storing of it.

* Firms should not proactively restrict processing of a data subject's personal data where this has not been requested, as that could mean the firm has failed to keep the personal data accurate or up-to-date.

* Firms should proactively delete data where they do not have grounds to process it, including where consent has lapsed and no other ground exists to justify retaining it.

* Firms should produce a data subject ‘scenario table' so they can have a clear policy on how they will handle data retention, right to restrict processing and right to erasure requests. Firms should look to obtain legal guidance where possible in relation to the specifics of their business.

Lawful processing: Questions for the wider community

* Do you agree with the premise that, as there is no clear limitation when a client can make a complaint, that it is necessary to keep all data to the extent that an advice firm could defend a legal claim?

* Do you agree the point at which a client agreement is signed is an appropriate juncture at which to assume a complaint could be made by the client?