Code Review Project | Consumer Policy Division

Central Bank of Ireland

(By email)

Re: - Consumer Protection Code Review – Discussion Paper

12th May 2023

Dear Code Review Team,

The Data Protection Commission (DPC) is responsible for upholding the rights of individuals as set out in the GDPR and Data Protection Acts 1988-2018 (Data Protection Acts) and enforcing the obligations upon data controllers. The DPC is appointed by Government and is independent in the exercise of its functions. The DPC does not approve any particular use of personal data but offers guidance as to the obligations and responsibilities of data controllers.

The DPC welcome the opportunity to provide observations on the October 2022 discussion paper regarding a review of the Central Bank of Ireland's (CBI) Consumer Protection Code (hereinafter referred to as "the Code"). Please note that the DPC is not going to comment on all of the discussion items in respect of the Code but only those items that overlap with the data protection framework. The DPC recognises that the Code is part of the CBI's regulatory functions and is used for investigation and enforcement action. In that regard, the DPC does not wish to interfere with the CBI regarding the exercise of its regulatory functions. Neither does the DPC expect the CBI to have responsibility for, or the regulatory function under the Code, to apply the GDPR regulatory provisions other than what is required from the CBI in its own collection and processing of personal data. The function of regulating the GDPR and Data Protection Acts rests solely with the DPC. However, the Code does overlap on a few issues, which we have highlighted below and which require further consideration in the Code itself and possibly in the guidance document accompanying it. This is to ensure that any instruction in the Code operates in a manner that also complies with the data protection legislation and that regulated entities do not use the Code as a means to deflect or override data protection regulatory requirements.

For clarification, the terms "Consumer", "Data Subject", "Customer" and or Individual or Person, referred to in this document shall all be assumed to refer to each other even though each has different statutory definitions. We note that there is no statutory definition of a "*Potential Customer*" which may need further clarification in the revised Code.

In addition, any reference to a regulated entity, data controller, business, company, SME, Insurance undertaking or intermediary shall be assumed to be one and the same, even though there may be different statutory definitions.

1. **Overlap and potential conflict in the Code with data protection legal requirements and fundamental rights of individuals under the GDPR.**

There is an issue regarding a "*potential*" customer who provides confidential information in the quotation process for a financial credit or an insurance policy agreement, but then that person does not proceed to enter a contract with the regulated entity and has no legal relationship with that entity, after receiving a quote.

Following a number of complaints to this office (see Appendix A below with case study examples), the DPC is concerned about the quotation process that gathers a vast amount of personal data on the consumer.

The DPC notes that this collection process is required under Chapter 5 of the Code prior to the regulated entity offering, arranging or providing a product or service appropriate to that consumer. In this regard, the Code also outlines the types of personal data required, which could include, where relevant, the age, health status, dependents, employment status, income and savings of that consumer. This may be relevant and necessary information for the regulated entity to do its "*assessment of suitability*" of the potential customer's needs for a relevant credit or insurance product. The DPC has no issue with this processing on a fully informed consent basis, provided that the data controller meets the conditions of consent as set out in **Article 7 of the GDPR** and ensures processing is solely for the purpose of providing the quotation to the consumer for the relevant product as required by the **Article 5** '***Purpose Limitation***' principle of the GDPR.

It is also important that the assessment of suitability process is conducted with full transparency to the consumer and does not have any hidden data matching or profiling of the consumer or that the person would be unaware that this is being done without that person first being fully informed. For example, digital processing can have multiple processing activities working in the background through the use of algorithms, cookies or other software applications that are not visible to the consumer but which can amalgamate large volumes of an individual's personal data. Failure to inform a consumer of additional processing taking place or the associated risks attached may render the consent of a consumer invalid. Finally, any such processing for the purpose of its assessment of suitability should comply with **Article 5** '***Data Minimisation***' principle of the GDPR and be adequate, relevant and limited to what is necessary only.

An issue may occur with the processing of personal data when a consumer either does not complete the quotation process in full or where they decline the quotation offer and cease to have any further contact with the Regulated Entity regarding that specific quotation process. In this regard, **Article 5** '***Storage Limitation***' principle of the GPDR applies as it requires that the personal data shall be kept in a form that permits identification of the data subject for no

longer than is necessary for the purposes for which the personal data is collected. As the quotation process has ended with no contractual agreement between the parties, the entire personal data and other confidential information that the consumer provided should be deleted by the regulated entity after a reasonable short period of time (i.e. after a relevant cooling off period) has elapsed, unless it can identify a lawful basis for the retention of personal data (and that the rationale or period for retention is appropriately notified to the consumer at the time of the collection of personal data).

However, if the regulated entity did comply with the Storage Limitation principle as required by the GDPR, then there is a strong possibility that the potential customer could be affected in exercising other rights that they may have, i.e. making a complaint to another Regulator, such as the Financial Services and Pensions Ombudsman, or under the Equal Status Acts or to the CCPC. This, in turn, could be a detriment to the regulated entity that, having deleted the data, then it now has no information to defend itself against any such potential complaints, for possible refusal of a service or for possibly unfairly assessing the suitability of the individual to a particular product, or for an automated decision that has produced legal effects on the consumer that had no human intervention for the regulated entity with that consumer.

To further complicate matters, the consumer has the fundamental data protection right, under **Article 17 of the GDPR *to erasure or a right to be forgotten***. Many of the complaints (as per Appendix A) that the DPC has received are under this provision which states as follows:-

> *1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*
>
> *(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
>
> *(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*
>
> *(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*
>
> *(d) the personal data have been unlawfully processed;*
>
> *(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

These rights are fundamental, especially where there has been no contract entered into by the consumer who may have done several online quotation processes with various different companies and no longer requires their personal data to be retained by the regulated entity and has no legitimate reason to make a legal complaint to any other regulator such as the Financial and Pensions Ombudsman etcetera. Therefore, if any of the above fundamental data protection rights are exercised by a consumer, then an anomaly is created, and a potential conflict exists for the entity regarding complying with the GDPR or complying with the Code. However, there are exemptions to the right which are not absolute, as follows:-

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) 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;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Possibly subsections (b) and/ or (e) are the most relevant in the quotation scenario and will require further consideration. In this regard, the DPC suggest that the updated Consumer Protection Code should ensure that no consumer rights are overridden by or take precedence over the GDPR fundamental rights to object/be forgotten/erasure. However, to balance this and ensure that regulated entities can comply with the many different consumer laws and possibly protect themselves from potential regulatory investigation and enforcement or civil legal claims, there should also be a possibility that the regulated entity can obtain from the consumer confirmation that the person also will acquiesce in their other consumer rights such as complaints to the Financial and Pensions Ombudsman or CCPC etc. This could possibly alleviate the potential of claims taken against the regulated entity for deleting the data gathered under the quotation process for a person who does not become a customer of the entity. If any record is to be retained by the entity, it could be a limited record in the

"*Statement of suitability"* that the Quotation process was deleted and that the entity received a confirmation from the individual that they were acquiescing on any other legal remedy that they may have had, in order for their fundamental right to erasure and to be forgotten, to be implemented in full.

Finally, it is in the consumer's best interests to shop around to ascertain the best quotation for a mortgage, credit or insurance policy. However, it should be a condition in the Code that the consumer should not be negatively impacted for supplying very confidential sensitive personal data about health, income and dependants, including any special categories of personal data, to a company that it will not be a customer with and which said the company will be retaining the data without a fair process for deletion of same that would be in compliance with Article 17 of the GDPR.

2. Digital Marketing

The ePrivacy Regulations - *the European Communities (Electronic Communications Network and Services) (Privacy and Electronic Communication) Regulations 2011 (S.I. 336 of 2011)* (due to be amended by EU Regulation) apply in full, regarding any guidance on electronic marketing.

We note the Code provisions in 3.40 and 3.41 regarding telephone contact and to the reference in the Guidance Note, dated May 2021, that these provisions are "*… without prejudice to any other obligations a regulated entity is subject to, including without limitation, under the Data Protection Acts 1988 and 2003."* Please note this is incorrectly referenced and should be changed to Data Protection Acts 1988 - 2018, The General Data Protection Regulation (GDPR) and associated data protection laws *such as the European Communities (Electronic Communications Network and Services) (Privacy and Electronic Communication) Regulations 2011 (S.I. 336 of 2011).*

For further information, please find the following guidelines.

In addition, we strongly recommend that a statement reminding regulated entities that the Code provisions are without prejudice to other obligations, such as their data protection obligations, is included in the updated Code. E-Privacy Regulations take precedence over the provisions within the Code, and this should be set out clearly in the revised Code.

Similarly, there is an obligation on data controllers when using digital technology, software, or web forms, in the on-line quotation process that they follow the DPC guidelines on the use of Cookies

3. Knowing the customer requirements (Chapter 5)

We note that the guidance document of May 2021 has the following under paragraph 4.1:

"*Reminder regarding compliance with Data Protection requirements when gathering information from consumers.*

It should be noted that, in order to comply with data protection requirements, information gathered from consumers by a regulated entity in compliance with the 2012 Code and, in particular, the Knowing the Consumer requirements (Chapter 5) should be used for the sole purpose for which it was gathered, for example assessing suitability. This data cannot subsequently be processed for other purposes, such as identifying marketing opportunities."

The DPC welcomes this statement and would like to see it set out in the Code itself either as a paragraph or a footnote. Please note that the **Purpose Limitation principle under Article 5 of the GDPR** is not just in relation to "*Identifying Marketing opportunities*", but is required for all personal data that is…

"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."

Furthermore, if a data controller/regulated entity does wish to explore marketing opportunities with an individual, then that should only be done under the legal basis of the fully informed, autonomous consent of the consumer, as per Article 6.1 (a) of the GDPR and as required by the ePrivacy Regulations. This should be in satisfaction of and in conjunction with the conditions to support consumers' best interests.

4. Retention of contracted customer personal data for regulatory purposes under the Code

Under Article 5 principles of the GDPR for Purpose Limitation and Storage limitation, the requirements for retention of data that includes personal data should only be retained by regulated entities for specified defined regulatory purposes. The retention period usually starts on the cessation of a contract, mortgage or insurance policy. The Purpose limitation for retention is normally for the regulatory purpose of the individual either exercising a regulatory right of complaint or for the Data controller / regulated entity to defend any allegations of improper conduct or regulatory investigation or civil claims or criminal charges. The retention period is for exactly the time period prescribed by Legislation and should not be for 6 years, *plus 1 year*.

To comply with these principles, the data controller should compartmentalise the storage of data for regulatory purposes only so that there are safeguards, in situ, that the personal data is not further processed for any other purpose. The data should be restricted to access for only 'a case by case', basis depending on whether or not a complaint or an investigation could be initiated. Other personal data of customers should not be accessed or further processed if not necessary.

5. Digitalisation

We agree with the comments as set out in the discussion paper regarding the following extracts:-

"*The use of Big Data and AI also presents risks to consumers, for example in terms of information asymmetries. From a consumer perspective, these asymmetries, facilitated by algorithmic profiling which is invisible to consumers, have the potential to create an inequality where a firm has much greater knowledge about the consumer, affecting how the firm markets products, prices products for the consumer and ultimately sells to the consumer. Used inappropriately, it could facilitate the exploitation of consumers, including those who are less familiar with technology, and enable unfair profiling Online Delivery of Credit - . The availability of and ease of access to credit can increase the risks posed by irresponsible lending for instance through aggressive and unsolicited marketing driven by on-line tracking and profiling, which can entice consumers into easily and quickly accessible loans."*

"The internet and social media represent a deeply data-rich and data-driven environment. This allows firms to access detailed information about the lives and lifestyles of consumers who, often unwittingly, provide information about themselves to internet service providers, which can be sold to other firms including financial services firms. This allows firms to directly target products and services to individual consumers based on certain data characteristics."

"There are risks associated with digital profiling, as consumers may not be aware of the extent to which the content they see is targeted or personalised to them. They may assume the products advertised to them are the most suitable based on the information they have provided when, in fact, they may be the most expensive products which are deemed by the product provider to be of interest to the consumer."

"Consideration needs to be given to the extent to which financial services firms can be allowed to use personal data, particularly big data and techniques such as machine learning which are enabled by such data, where significant imbalances between firms and consumers already exist."

"We expect that digital platforms are designed with the consumer's interest in mind. We expect firms to ensure that digital platforms are easy to navigate, to use and to understand, ensuring that consumers do not need specialist knowledge in the use of such technology. It is important to ensure that certain cohorts of consumers, including those with poor digital literacy, are not excluded through poor design. The use of technology by consumers should serve their interests and not be viewed as an opportunity to take advantage of their behavioural vulnerabilities, or to increase information asymmetries between consumers and firms."

The DPC would expect that the relevant entities using new technologies to process consumer's personal data would perform a **Data Protection Impact Assessment** as required by **Article 35 of the GDPR**. Furthermore, consideration should be given to privacy-enhanced technology that implements the necessary privacy-by-design features to protect the consumer from any unnecessary, irrelevant or unlawful processing of their personal data.

6. Vulnerable persons and assisted decision-making

The DPC notes the following regarding, *Dealing with Individual Cases*.

"*The Code obliges firms to provide those identified as vulnerable with such reasonable arrangements and/or assistance that may be necessary to facilitate him or her, in their dealings with the firm. Staff of financial services firms need to be able to recognise and respond to vulnerability. They need to know when it is appropriate to seek additional support within the firm for customers depending on their circumstances. They should be empowered to seek that support and appropriately record information, while respecting the privacy and autonomy of the individual, to ensure future engagement with the customer takes account of their particular circumstances. Firms need to consider the organisational arrangements that need to be put in place to support customers in vulnerable circumstances.*"

The DPC fully agrees with this statement. But we believe the development of structured guidance for all service entities when dealing with a vulnerable customer or a trusted person or third party acting on behalf of the vulnerable person (i.e. Solicitor, Accountant, persons appointed under the Assisted Decision Making (Capacity) Act 2015, as amended) would help ensure a consistent application of best practice. In this regard, we recommend that consideration should be given to the option of producing a **Code of Conduct under Article 40 of the GDPR**. The purpose of this Code of Conduct would be to resolve any difficulties that the service industries experience when dealing with a vulnerable customer or that persons representative and provide clear rules and procedures as to how the industry can interact and deal with relevant scenarios that they may face, when collecting or disclosing personal data of a vulnerable person and processing said data in a fair and transparent manner. This is a possibility that the Central Bank of Ireland, in conjunction with its functions under the

Consumer Protection Code, may wish to consider further and, in addition, whether or not it wishes to be considered as the independent body that monitors the Code of Conduct as set out in Article 41 of the GDPR. For further information on Codes of Conduct, please see here.

Finally, the DPC looks forward to the second stage consultation process. We are available to discuss and elaborate on any of the issues as set out above.

Yours faithfully,

Garrett O'Neill

Assistant Commissioner

APPENDIX A

From DPC website page on case studies:

Case study 22: Erasure request and reliance on Consumer Protection Code

Following an unsuccessful application for a credit card, the data subject in this case sought to have their personal data erased under Article 17 of the General Data Protection Regulation (GDPR). When the erasure request was refused by the data controller, the data subject raised concerns with the DPC that their personal data was being unlawfully retained. The DPC engaged with the data controller in order to assess the reasoning for such refusal.

In response to the data subject's initial erasure request, the data controller stated in line with provision 11.6 of the Consumer Protection Code 2012 and their Privacy Policy and Cookies Statement they had a legal obligation to retain the information provided. The data controller went further to explain that the personal data provided in the application would be retained for a period of six years from the date on which the service was provided.

As part of its examination, the DPC engaged with the data controller and requested a response to the complaint. The data controller stated that they were relying on Article 6(1)(c) of the GDPR to retain the personal data whereby processing is necessary for compliance with a legal obligation to which the data controller is subject. The data controller in this case was also subject to the Consumer Protection Code 2012 (CPC). On this basis the data controller relied on this lawful basis for the refusal of the erasure request. Under Article 17(3)(b) of the GDPR, a data subject's right to erasure does not apply and may be restricted where the processing is necessary for compliance with a legal obligation.

For reference, the CPC is a set of rules and principles that all regulated financial services firms must follow when providing financial products and services to consumers and was published

by the Central Bank of Ireland in compliance with section 117 of the Central Bank Act 1989. Under section 117(4) of the Central Bank Act 1989, it is an offence for a regulated financial firm to fail to provide the Central Bank with information to demonstrate compliance with the CPC.

Provisions 11.5 and 11.6 of the CPC require data controllers to retain the records of a consumer for six years after the date on which a particular transaction is discontinued or completed. The required records include but are not limited to: all documents required for consumer identification; the consumer's contact details; all correspondence with the consumer; all documents completed or signed by the consumer. The data subject contested this reliance as no service was provided, therefore they were of the view they were not a consumer and as such felt the data controller had no legal right to maintain the personal data. The CPC defines a consumer and includes where appropriate, a potential consumer. In addition to this, the data controller stated when the data subject applied for a credit card, the consideration of the application and subsequent decision was deemed a service.

Under section 109(5) (c) of the 2018 Act, the DPC advised the data subject that within the meaning of the CPC they were classified as a potential consumer. As a result the data controller is legally obliged to retain the personal data for a period of six years. The DPC did not consider any further action necessary at the time of issuing the outcome.

Case study 28: Retention of data by a bank relating to a withdrawn loan application

The complainant in this case had made a loan application to a bank. The complainant subsequently withdrew the loan application and wrote to the bank stating that they were withdrawing consent to the processing of any personal data held by the bank relating to the loan application and requesting the return of all documents containing the complainant's personal data. In response, the bank informed the complainant that it had stopped processing all of the complainant's personal data, with the exception of data contained in records which the bank stated it was required to retain and process under the Central Bank of Ireland's Consumer Protection Code. The complainant was not satisfied with this response, and argued, in their complaint to this Office, that in circumstances where the bank had obtained the complainant's personal data on the basis of the complainant's consent, the bank was not permitted to continue to process these data on a different legal basis (i.e. processing which is necessary for compliance with a legal obligation to which the bank is subject). The complainant also argued that the continued processing by the bank of their personal data was for a purpose which was not compatible with the purpose for which the data were originally obtained, in contravention of data protection legislation.

This office established that the bank was identified as the relevant data controller in relation to the complaint, as it controlled personal data which the complainant had provided to the bank when making a loan application. The data in question were personal data relating to the

complainant (consisting of, amongst other things, a completed loan application form and supporting documentation) as the complainant could be identified from it and the data related to the complainant as an individual. This office was therefore satisfied that the complaint should be investigated to determine if a breach of data protection legislation had occurred.

During the course of the investigation of this complaint, this Office reviewed the bank's loan application form, which provided that, by signing the form, a person consented to the bank storing, using and processing their personal data for a range of purposes, including to process applications for credit or financial services. However, this Office noted that the purposes for which the complainant had given their consent did not include processing for the purpose of compliance with the bank's legal obligations generally, and specifically did not include the processing of the complainant's personal data for the purpose of compliance with the Consumer Protection Code. Accordingly, this office considered that at the time of collection of the complainant's personal data the Bank did not claim to rely on consent as the legal basis for the collection and processing of the complainant's personal data in order to comply with its legal obligations. Rather, this office considered that the bank could validly rely on the lawful basis that the processing was necessary in order to take steps at the request of the data subject prior to entering into a contract.

This Office noted that where a loan application is subsequently withdrawn or unsuccessful and the bank does not enter into a contract with the applicant, the retention of personal data relating to the loan application can no longer be on the basis that the processing was necessary in order to take steps at the request of the data subject prior to entering into a contract, as there is no longer the possibility of entering into a contract with the data subject. As such, the bank identified a separate legal basis for the retention of the complainant's personal data relating to the loan application, namely that this processing was necessary for compliance with a legal obligation to which the bank was subject.

This Office noted that the Consumer Protection Code obliged regulated entities to retain details of "individual transactions" for six years after the date on which the particular transaction is discontinued or complete. This Office considered, however, that a loan application which is subsequently withdrawn or ultimately unsuccessful is not a 'transaction' for the purpose of the Consumer Protection Code. This Office then noted that the Consumer Protection Code also obliged regulated entities to retain "all other records" for six years from the date on which the regulated entity ceased to provide any product or service to the consumer, including potential consumer, concerned. However, this Office did not consider that records relating to a loan application which is subsequently withdrawn to fall within the scope of this requirement under the Consumer Protection Code either. Accordingly, this Office considered that it was not necessary for the bank to retain personal data relating to the complainant's withdrawn loan application for the purpose of compliance with its legal obligations under the Consumer Protection Code, and considered that the bank had not

identified a lawful basis under data protection legislation for the retention of the complainant's personal data relating to their loan application.

Under Article 6 of the GDPR, data controllers must have a lawful basis for any processing of personal data. The available lawful bases include that the data subject has given consent to the processing of their personal data for one or more specific purposes, that the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract, and that the processing is necessary for compliance with a legal obligation to which the data controller is subject. Data controllers should note also that the processing of personal data for purposes other than those for which the personal data were originally collected is only allowed where the processing is compatible with the purposes for which the data were initially collected.