



# ABI data principles for supporting vulnerable customers



## Background

The insurance and long-term savings industry takes care of customers with different needs or those in vulnerable circumstances on a day-to-day basis. The industry has been striving to deliver the most suitable customer service and cater to individual needs. In the past several years, the ABI has published different codes and guidance to improve the treatment of vulnerable customers, or those with specific needs, in different parts of the business. These include:

- ABI Mental Health and Insurance Standards <sup>1</sup>
- ABI's Guide to Identifying and Supporting Vulnerable Customers in the Long-term Savings Market <sup>2</sup>

Coinciding with the FCA's work in this area, including the launch of its Guidance for firms on the fair treatment of vulnerable customers <sup>3</sup>, the ABI has set up a cross-industry Vulnerable Customers Working Group so that firms can share their experience and develop a more consistent approach towards issues across the industry. This document captures the suggestions, queries and ideas from the group's discussions, in order to share good practice and demonstrate the industry's commitment to this issue.

---

1. <https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/health-insurance/mental-health-standards/>  
2. [https://www.abi.org.uk/globalassets/files/publications/public/its/abi\\_addressing\\_customer\\_vulnerability\\_final2.pdf](https://www.abi.org.uk/globalassets/files/publications/public/its/abi_addressing_customer_vulnerability_final2.pdf)  
3. <https://www.fca.org.uk/publications/finalised-guidance/guidance-firms-fair-treatment-vulnerable-customers>

## Objectives

Identifying, recording and managing information relating to vulnerability is key to providing a positive customer experience. There are benefits of insurance and long-term savings firms being aware of vulnerable customers' needs, and it is a crucial step in ensuring customers are effectively supported throughout the customer journey. This requires firms to approach the recording of vulnerability data in an effective, responsible and pragmatic way.

This document seeks to support firms across the insurance and long-term savings sector and is complementary to the ABI's existing good practice guidance. This document sets out general principles of how firms operating across our sectors can approach the needs of vulnerable customers, specifically when obtaining and processing their personal data, and aims to support firms in doing so.

The protection of vulnerable customers is integral to the way that regulators are approaching their responsibilities within the wider social and economic situation. This document also aims to set out our recommended general principles for applying this regulatory focus on vulnerable customers and to remind firms of the key data protection requirements that are triggered when a customer requires additional support.

### Disclaimer

These principles are designed to support firms to follow the FCA's guidance for firms, they are not intended to provide regulatory or legal advice nor suggest that firms should take any particular course of action to meet their regulatory and legal obligations.

The principles do not represent an example of acceptable market practices or standards in the context of the fair treatment of vulnerable customers and adherence to the FCA's guidance for firms. The principles will need to be interpreted in the specific context of each firm and each firm will need to exercise their own judgement about how to treat their vulnerable customers fairly.

These principles were published on 4 May 2021 and take effect from that date.

---

## Key considerations

This document only sets out good practice in relation to supporting the disclosure and identification of additional customer needs. At every point of the customer journey, firms must continue to comply with data protection law and other legal requirements on data collection and processing. For example, by only collecting information about a customer's vulnerability status where it is appropriate, strictly necessary to understand and accommodate the needs of the vulnerable customer, and where firms have a lawful basis for processing this data<sup>4</sup>. When there is uncertainty, firms might want to obtain their own legal advice, or consult data privacy employees in their own organisations. There are a number of other key considerations that should be made at every step of the journey, as a foundation to the additional points of good practice below:

- Firms could also ensure that customers are made aware of how their data is used and managed, with timely, transparent and concise communications when capturing information. Alongside these principles, firms could work with their data privacy employees when designing, implementing and following their own vulnerable customer policies.
- During the recording process, firms could choose only to record objective information at point of disclosure, not their opinion, and explain to the customer why they are recording this information, as appropriate. This could be achieved by recording statements using the customer's own words, repeating to the customer what will be recorded, with a focus on recording the needs or adaptations that the customer asks for rather than an assumed condition or category.
- Firms should ensure they have a lawful basis for processing the data if a customer, who may be considered vulnerable, discloses a condition or situation. Finally, firms may wish to regularly review their processes and make necessary changes to satisfy changing customer needs and regulatory requirements.

---

4. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

# Principles

## 1: Identify vulnerability and additional needs

**Aim: Ahead of considering data recording, firms put in place measures to identify customers who require additional support.**

### To achieve this, firms could:

- a. Implement and follow their existing vulnerable customers policies to support customers who may be vulnerable.
- b. Include a firm-level approach within their vulnerable customers policies, to help identify these customers across the spectrum of risks. To do so, firms could consider structuring their approach around the drivers of vulnerability highlighted by the FCA in its guidance for firms.
- c. Ensure customers are supported at each communication touchpoint, particularly where a firm's products or business model makes infrequent customer contact more likely. Firms could also offer various communication channels through which customers can notify providers of any challenges faced.
- d. Work with intermediaries or other third-party suppliers who engage with the customer (where a firm's distribution model relies on this), so that they employ similar strategies to identifying and recording vulnerability status. This information should only be shared in line with regulatory and legal requirements.
- e. Deliver an ongoing commitment to supporting staff to

be attuned to the drivers of vulnerability, through the provision of regular training and other resources.

- f. Ensure particular consideration is given to special category data <sup>5</sup>, such as health data, and how this is captured. Further good practice on this is provided in the FCA's finalised guidance <sup>6</sup> for firms.

## 2: Embed a consistent approach to recording vulnerability data

**Aim: Firms provide a consistent and positive experience to all their customers across all product lines whenever possible.**

### To achieve this, firms could:

- a. Use the definition of a vulnerable customer set by the FCA <sup>7</sup> consistently across their firm when recording data, while flexibility may be required to adapt to particular product lines or business areas. The ICO's definition of 'vulnerable individual' <sup>8</sup> should also be considered in matters related to data protection.
- b. Review training needs for frontline staff regularly to ensure good practice, taking into account legal and regulatory developments.
- c. Ensure that their messaging in relation to data recording is consistent across different communication channels (e.g. telephony, online chats, emails, letters), and provisions to cater for vulnerable customers are in place.
- d. Evaluate how well their systems speak to each other, and whether there is scope to update these.

## 3: Support customers to disclose their needs

**Aim: Customers feel supported, confident and never pressured to disclose information in relation to their personal circumstances, so that providers can offer appropriate support to those who are vulnerable and/or require additional support. Customers are informed of the benefits of doing so and have trust in providers managing data on their vulnerability status.**

### To achieve this, firms could:

- a. Consider what barriers may currently be in place within their firms that discourage disclosures, and seek to remove these.
- b. At point of disclosure, inform their customers about the processes they have put in place to support customers and communicate how information relating to vulnerability status will be treated and used to support them.
- c. Ensure frontline staff are trained to identify any potential vulnerability triggers, and that they are equipped with the appropriate tools and training to build trust and support disclosures from customers.
- d. Explore how case studies from within their firm can be utilised to facilitate training and ongoing support for staff. The latter should only be used if all personal data is removed and anonymised.
- e. Where appropriate, seek to raise the customer's

5. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

6. <https://www.fca.org.uk/publications/finalised-guidance/guidance-firms-fair-treatment-vulnerable-customers>

7. *Who are vulnerable customers?*, pp. 61, <https://www.fca.org.uk/publication/guidance-consultation/gc20-03.pdf>

8. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when11>

awareness of additional support services that may be available from other organisations at point of disclosure and during ongoing discussions in relation to the specific vulnerability.

- f. Provide additional opportunities within the customer journey for customers to learn about the provider's approach to vulnerability and to inform the firm about their needs, for example through the website, annual benefit statements and Interactive Voice Response.

#### 4: Provide tailored support using vulnerability data

**Aim: Customers' vulnerability status and records are used, if appropriate, to spot signs of vulnerability and inform support needed and the service offering, with robust data protection in place.**

##### To achieve this, firms could:

- a. Consider if systems can be customised or amended to record additional needs where legacy systems prevent adequate data recording or access.
- b. Enable staff supporting customers to have access to information that the firm holds or obtains from customers that indicates that the customer may require additional support. If possible, the information should be easily visible to these staff.
- c. Ensure customer data is only accessible by staff within firms who may need it and that staff can only see data that they need to see.
- d. Provide vulnerable-customer focused data protection training and other necessary information to ensure staff can explain to customers how data is handled and used in line with data protection principles.

- e. Analyse vulnerability data, existing research and other data sources to improve the understanding of their customer base and identifying characteristics of vulnerability in individual customers. The insight could be used to provide tailored and/or additional support or to improve products and processes by design.
- f. Regularly review the storage of data and the length of time that data is retained on file. Only keep data for as long as it is needed, in line with financial services regulations and data protection law and/or principles relating to processing of personal data, including purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

#### 5. Keep customers in mind throughout the process of recording data

**Aim: Firms can demonstrate a considered approach to recording vulnerable customer data. Effective and appropriate customer service is provided throughout the process of data recording in relation to vulnerability.**

##### To achieve this firms could:

- a. Regularly review their approach to data recording and stay up to date on data recording good practice, innovations and solutions in the market.
- b. Focus on recording the reasonable adjustment needed to accommodate the needs of the vulnerable customer as opposed to the cause of the vulnerability.
- c. Where recording the reasonable adjustment is not sufficient to understand the needs of the customer, limit any additional information recorded to the impact of the vulnerability as opposed to the cause of the vulnerability.

- d. Review and keep records of the support offered to vulnerable customers to improve future services.
- e. Present what the firm holds about a customer in relation to their vulnerability status or needs in a clear, understandable and accessible format, when a customer requests it. Customers should be made aware of their data subject rights.
- f. Treat data recording holistically in line with a firm's overall approach to supporting vulnerable customers and aligning to the regulator's guidance.
- g. Prioritise the additional needs that customers may require at a certain time, noting that these may be temporary and may not deem a customer "vulnerable".

#### 6. Facilitate third-party disclosures

**Aim: Family members and other third parties are able to communicate a customer's additional needs to a firm, while the customer remains protected and supported.**

##### To achieve this, firms could:

- a. Have procedures in place for processing and working with attorneys, when a customer has power of attorney or court order of deputyship in place.
- b. While approaches may differ from firm to firm, have a consistent and measured approach, with appropriate levels of due diligence, when disclosures are made by third parties that do not have power of attorney.
- c. Be mindful of the risks involved with liaising with third parties, and ensure staff are trained to recognise signs of abuse or scams. Firms may wish to work with charities to ensure appropriate protections are in place.