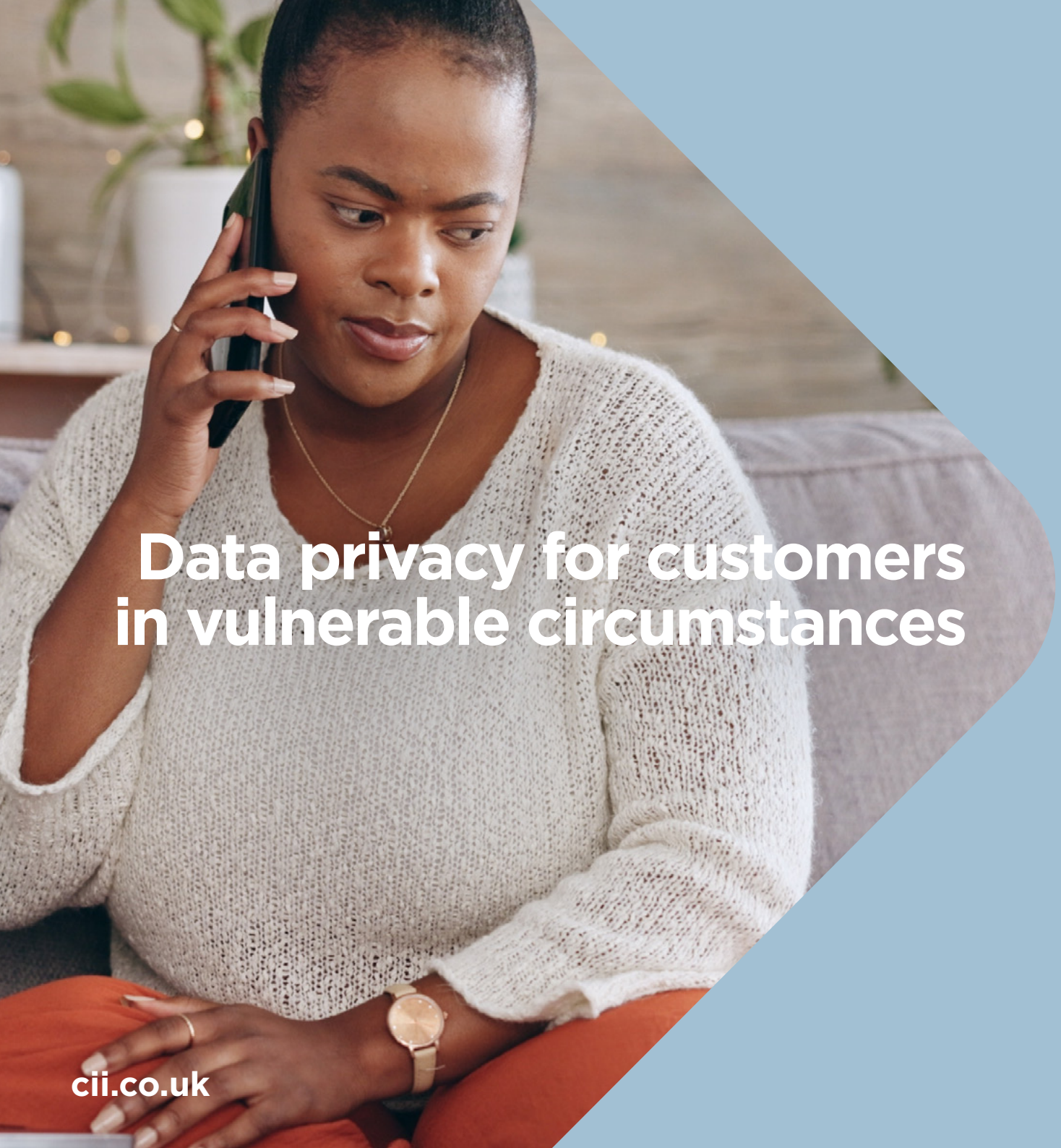

Chartered Insurance Institute

Standards. Professionalism. Trust.

Data privacy for customers in vulnerable circumstances

A practical guide for insurance and personal finance firms

cii.co.uk

Contents

Foreword 3

Executive summary 4

PART 1: CONTEXT AND PRINCIPLES 5

1 Introduction 5
- 1.1 Regulatory background 5
- 1.2 Who is this guidance for? 6
- 1.3 Purpose and scope 6
- 1.4 Data privacy aim: building trust 7

2 Privacy principles for vulnerability data management 8

PART 2: VULNERABILITY DATA REQUIREMENTS 10

3 Why process vulnerability data? 10
- 3.1 First purpose: to provide appropriate support and prevent harm 10
- 3.2 Second purpose: to meet outcomes reporting requirements 11
- 3.3 Third purpose: to drive product and service improvements 12

4 What vulnerability data should be processed? 13
- 4.1 Collect data on all customers 13
- 4.2 Record sufficient information for effective support 13

5 How should vulnerability data privacy be implemented? 15
- 5.1 Gradual vulnerability data enhancement 15
- 5.2 Use proactive and reactive methods to identify vulnerability 16
- 5.3 Treat all vulnerability data as special category data 17
- 5.4 Integrate vulnerability data privacy into existing processes 18
- 5.5 Centralise decisions on vulnerability data management 18
- 5.6 Ensure systems are fit for purpose 18

PART 3: ESTABLISHING POLICIES 19

6 Lawful basis for processing 19
- 6.1 Establishing the purpose for processing 19
- 6.2 Default lawful basis: explicit consent Article 9(2)(a) 20
- 6.3 Alternative lawful bases 21
  - 6.3.1 Legitimate interest - Article 6(1)(f) 21
  - 6.3.2 Vital interest - Article 9(2)(c) 21
  - 6.3.3 Legal Claims and Judicial Acts - Article 9(2)(f) 22
  - 6.3.4 Substantial Public Interest - Article 9(2)(g) 22

7 Embedding vulnerability into data protection policies 25
- 7.1 Integration with existing policies 25
- 7.2 Documenting how vulnerability data is processed 25
- 7.3 Privacy notices 25

PART 4: OPERATIONAL DATA MANAGEMENT 26

8 Managing vulnerability data in practice 26
- 8.1 Collect vulnerability data 26
  - 8.1.1 Direct data collection (customer-led) 26
  - 8.1.2 Indirect data collection 26
- 8.2 Record vulnerability data 27
  - 8.2.1 Recording inferred data 27
  - 8.2.2 Record the right amount of information 28
- 8.3 Keeping data accurate 30
  - 8.3.1 Why data accuracy matters 30
  - 8.3.2 Ensuring data accuracy at the point of recording 30
  - 8.3.3 Keeping data up to date 32
  - 8.3.4 Historical records 32
- 8.4 Retention 34
- 8.5 Storing vulnerability data safely 34
- 8.6 Responding to customer requests regarding vulnerability data 35
  - 8.6.1 Right to erasure (the right to be forgotten) 35
  - 8.6.2 Data Subject Access Requests (DSAR) 36

9 Sharing vulnerability data 38
- 9.1 Tiered access model 38
- 9.2 Sharing within firm 39
- 9.3 Sharing across the distribution chain 39

10 References 40

11 Appendix: Lawful bases for processing vulnerability data. A scenario matrix. 41

Foreword

The Consumer Duty has rightly placed good customer outcomes at the heart of how firms must operate, with particular focus on those in vulnerable circumstances.

Across the sector, there is a clear commitment to meeting this expectation. Yet many firms remain uncertain about how to handle sensitive data in a way that is both effective and compliant, and this uncertainty can hold back progress.

This guide exists to address that challenge. The Financial Conduct Authority (FCA) and Information Commissioner's Office (ICO) have been clear that UK data protection laws do not prevent firms from processing vulnerability-related data where it is necessary to support good outcomes. The issue is not the regulation itself, but the practical complexity of working confidently across regulatory frameworks, and a perception that information sharing cannot be done. Providing clarity on how it can be done — appropriately and responsibly — is therefore essential and will also help to further build consumer trust.

I am grateful to all those who have contributed their expertise and insight to this work. I commend this guidance to firms across the sector and encourage its use as a practical foundation for embedding consistent, customer-centred practice.

Matthew Hill,
CII Chief Executive

1 Executive summary

The FCA's Consumer Duty requires firms to understand and support customers in vulnerable circumstances, necessitating the collection and management of substantial amounts of sensitive personal data. This creates a complex intersection with UK data protection requirements that many firms struggle to navigate effectively.

Uncertainties on how to approach consent that have led some firms to avoid systematic vulnerability data processing undermine both consumer protection and legal compliance.

The reality is that UK data protection laws don't prevent vulnerability data processing. When done for legitimate purposes, like supporting vulnerable customers, such processing is lawful and supported by the ICO.

This guide translates legal requirements into operational practices through clear explanations, decision-making tools, real-world examples and templates. It serves compliance officers, data protection officers, vulnerability leads and operations managers across insurance, financial advice, broking and the wider distribution chain.

While this guide represents good practice, it is not legal advice. Firms should consult their Data Protection Officers (DPOs) for specific applications.

PART 1: **CONTEXT AND PRINCIPLES**

1 Introduction

1.1 Regulatory background

The FCA Consumer Duty requires firms to understand their customers in vulnerable circumstances, and:

a) support each customer to prevent harm

b) monitor the circumstances of the customer over the lifetime of the product

c) improve their products and services and

d) maintain records of these activities as proof

This requires the storage and management of significant amounts of data, which needs to be done in a manner that is consistent with UK data protection laws.[1]

CII research has identified a range of specific implementation challenges firms encounter when managing vulnerability data under the FCA's Consumer Duty while maintaining compliance with UK General Data Protection Regulations (UK GDPR)[2] and the Data Protection Act 2018 (DPA 2018), including:

Challenge	What firms struggle with
Customer engagement	Creating environments where customers feel safe sharing vulnerability information
Permission and consent requirements	Understanding when and how to obtain permissions for processing personal data and whether consent remains the appropriate lawful basis for processing
Transparency	Balancing disclosure obligations to the customer with the sensitivity of the information shared, including privacy notice requirements
Data minimisation	Reconciling UK GDPR's minimum data principle (Article 5(1)(c)) with essential and relevant vulnerability data processing
Data accuracy	Managing records when vulnerabilities change including obligations to rectify or update information
Retention policies	Determining appropriate storage periods, applying storage limitation principles and controls where required
Inferred vulnerabilities	Using behavioural or transactional data to identify vulnerabilities without explicit disclosure
Data sharing	Managing secure information flows between stakeholders, third parties, or within or across firms, while preserving customer trust
Preventing data-induced vulnerability	Ensuring that customers who are not inherently vulnerable are not rendered vulnerable by unclear data processing practices, inaccessible privacy communications, poor consent design, and terms and conditions

While firms may perceive UK data protection laws as a barrier to vulnerability data processing, the reality is that processing data for clear, lawful purposes is entirely legitimate, as stated in the *Joint FCA and ICO statement on regulatory expectations regarding firms' approaches to vulnerability-related data*.[3]

1. Appendix 1 of the FCA's FG21/1 Guidance for firms on the fair treatment of vulnerable customers, covers UK GDPR and DPA 2018 considerations.
2. UK GDPR is listed under the following act: Regulation (EU) 2016/679 of the European Parliament and of the Council
3. Financial Conduct Authority, Joint FCA and ICO statement on regulatory expectations regarding firms' approaches to vulnerability-related data (FCA, London 2026)

PART 1: **CONTEXT AND PRINCIPLES**

1.2 Who is this guidance for?

This guide is for all UK-regulated firms within the insurance and personal finance sectors, including product providers, distributors, and third parties that are material parts of the distribution chain. While focused on these sectors, many principles will apply across financial services more broadly.

Intended readers:

The guide has been developed for professionals responsible for implementing vulnerability management and data protection practices, including:

- **Data protection officers (DPOs)** overseeing lawful processing and UK GDPR compliance
- **Compliance officers** ensuring regulatory adherence across Consumer Duty and UK GDPR
- **Customer vulnerability leads** designing and implementing vulnerability support programmes
- **Operations managers** translating policy into day-to-day operational practice
- **Customer service managers** training teams and handling customer interactions
- **Risk and governance teams** assessing and managing data protection risks
- **Legal and regulatory affairs** interpreting regulatory requirements
- **IT leads** implementing technical data management solutions

Important notice:

This guide addresses common scenarios firms will encounter when managing vulnerability data and makes assumptions about common practices. Each firm should consult with their own DPO when determining the lawful basis for processing vulnerability data and how they manage personal data under UK data protection laws. This guide recommends good practice, not legal or regulatory advice.

1.3 Purpose and scope

This guide clarifies in practical terms how customer vulnerability-related data can be managed compliantly:

This guide covers:

- How to manage data to meet both UK data protection laws and Consumer Duty requirements
- Lawful bases for processing vulnerability-related data
- Practical data recording, storage, and sharing
- Responding to customer data requests
- System and process requirements
- Individual vulnerability data collected via direct customer engagement (bottom up)

This guide does NOT cover:

- What data is required for vulnerability management[4]
- Use of Artificial Intelligence (AI) in vulnerability data management
- Distribution chain data sharing protocols
- Broader aspects of Consumer Duty compliance
- Vulnerability data collected through surveys where no personal identifiable data is collected
- Inferred vulnerability data derived from transactional data

Terminology

The guide generally uses FCA terminology for consistency, with plain English explanations provided throughout. However, for ease of reading we refer to ‘vulnerable customers’ as shorthand for ’customers in vulnerable circumstances.’ Similarly, the guide refers to UK data protection laws as shorthand for UK GDPR and DPA 2018.

4. For more information, see Chartered Insurance Institute, Managing customer vulnerability in insurance and personal finance, a practical implementation guide (CII, London 2025)

PART 1: **CONTEXT AND PRINCIPLES**

1.4 Data privacy aim: building trust

Compliance with UK data protection laws forms the foundation of this guide. They establish the minimum standards firms must meet when processing vulnerability data. However, beyond regulatory compliance, this guide supports the overriding focus of the Consumer Duty:

building trust and transparency with customers

To this end, we've adopted the following 'trust' principles based on research from the Money and Mental Health Policy Institute and Money Advice Trust: [5]

Principle	What it means	Why it matters
Consumer control	Customers want to feel in control, even if they don't actively exercise it	The ability to have control (when they want it) engenders trust
Transparency	Customers knowing and understanding how and why their data is used reduces fear and uncertainty	Openness about data use builds trust

These principles inform our recommendations on the most appropriate methods for processing vulnerability data, good practice, and the regulatory obligations firms must meet.

In practice

When choosing between lawful bases for processing, consider not just legal compliance but also which approach best supports these trust-building principles.

5. Money and Mental Health Policy Institute and Money Advice Trust. A once in 24 years opportunity: 10 principles for designing vulnerable consumer data-sharing programmes (2024)

PART 1: **CONTEXT AND PRINCIPLES**

2 Privacy principles for vulnerability data management

The table below describes data protection principles and how they apply to vulnerability data management in actionable terms:

Data-protection principle	Plain-English meaning	Why it matters for vulnerable customers	Good practice
Lawfulness, fairness and transparency	Be open and honest. Only collect or use data when you have a valid legal reason and tell the customer, in words they understand, what you'll do with it.	Builds trust and encourages disclosure. Clear explanations reduce fear of discrimination and re-disclosure fatigue.	Use accessible and simple privacy notices and explanations at relevant points. Explain how vulnerability data helps customers get better support. During disclosure, where possible, explain what data is processed (subject to consent, if applicable) and why.
Purpose limitation[6]	Use it only for the reason you have said. Don't repurpose vulnerability notes for marketing or commercial gain.	Ensures sensitive details are processed solely to provide support or meet FCA duties, not to disadvantage the customer.	Don't use vulnerability data for commercial gain. Do use it for customer support and regulatory compliance.
Data minimisation	Record 'just enough.' No more. No less. Capture what you need to help the customer and to evidence compliance, nothing irrelevant.	Reduces risk of over-exposing health, life-event facts, capability or resilience information, and reassures customers who worry about oversharing. However, this does not mean firms should only maintain data they are currently using. Historic data may be maintained for the purpose of keeping accurate records, for audit purposes, and because the data may become relevant again in the future.	Record circumstances and support needs, not unnecessary medical history. However, you may maintain historical data for accurate records and audit purposes.
Accuracy	Keep data correct and up to date. Wrong or outdated data can harm a customer or deny them suitable help.	Contact data and life events may change. Regular reviews prevent stale or misleading information which can lead to poor outcomes.	Review vulnerability data at appropriate intervals. Update when circumstances change. Keep historical records for audit trails.
Storage limitation	Don't keep data longer than necessary. Set review or expiry triggers. When the vulnerability no longer impacts the customer amend the data (but retain the history).	Limits the chance of old, sensitive data resurfacing (e.g. in a Data Subject Access Request) when it's no longer relevant.	Maintain date of records and retain history. Set retention periods based on product lifecycles.
Integrity and confidentiality (security)	Protect data from loss, leaks or unauthorised use.	Vulnerable-customer data is sensitive. A leak could lead to harm.	Use role-based access. Encrypt stored data. Share only with those who need it.
Accountability	Be able to show your workings.	Demonstrates to regulators, and to customers, that the firm systematically safeguards those who are most at risk.	Maintain objective, robust records. Document lawful basis decisions. Train staff. Conduct regular audits. Fix mistakes quickly.

6. The Data (Use and Access) Act 2025 (DUAA) enables flexibility with the purpose limitation principle but only in limited circumstances, which should be clarified by your DPO.

PART 1: **CONTEXT AND PRINCIPLES**

Privacy principles checklist

As part of vulnerability management, ensure that your firm's processes:

- ✔ Have a lawful reason for processing data (Lawfulness)
- ✔ Inform the customer what you are doing with the data (Transparency)
- ✔ Ensure the data is only used for supporting them or regulatory compliance (Purpose Limitation)
- ✔ Record only what they need (Data Minimisation)
- ✔ Ensure data accuracy (Accuracy)
- ✔ Allow for data deletion at an individual level (Storage Limitation)
- ✔ Store data securely with restricted access (Security)
- ✔ Keep records to prove best practice (Accountability)

If you cannot tick each of these, stop and address this issue before proceeding to process the data.

PART 2: **VULNERABILITY DATA REQUIREMENTS**

3 Why process vulnerability data?

There are three distinct and interconnected purposes for processing vulnerability data. Firstly, to provide appropriate support and to prevent harm. Secondly, to meet reporting requirements. Thirdly, to drive product and service improvements.

While these purposes are a regulatory mandate under Consumer Duty requirements, they also reflect a commitment to doing right by customers. Understanding customer's circumstances enables firms to prevent harm, provide appropriate support, and build products and services that work better for everyone.

3.1 First purpose: to provide appropriate support and prevent harm

The purpose of collecting vulnerability data is to deliver appropriate support and prevent harm. A label such as 'dyslexia', for example, has little operational value on its own. Firms need to identify the specific harm a customer is susceptible to because of their circumstances (e.g. misunderstanding complex terms and conditions) and use that understanding to ensure communications are clear and not misleading, and that products and services remain suitable.

Example: dyslexia

Insufficient recording: 'Customer has dyslexia'

Effective recording:

- Circumstance: Dyslexia (moderate severity)
- Potential harm: Misunderstanding complex terms and conditions
- Support: Dyslexia-friendly communication formats, extra time to review documents, verbal explanation of key points, follow-up confirmation calls

Result: Customer receives documents in accessible format, with clear verbal explanations, reducing risk of misunderstanding policy terms.

Principle: Recording 'what' without 'why it matters' and 'what helps' fails to deliver effective support.

PART 2: **VULNERABILITY DATA REQUIREMENTS**

3.2 Second purpose: to meet outcomes reporting requirements

The Consumer Duty mandates that firms monitor customer outcomes to ensure that vulnerable customers receive outcomes as good as those received by non-vulnerable customers. This requires robust data management systems to:

- Compare outcomes between vulnerable and non-vulnerable customer groups
- Identify disparities where certain groups experience poorer outcomes
- Record information accurately to prevent customers from having to repeatedly disclose sensitive details

Example: target market analysis

An insurer undertakes analysis for a specific product.

Step 1: Identify customer groups for the product

- Customers with no identified vulnerabilities
- Customers experiencing a negative life event (e.g. recent loss of spouse/partner)
- Customers with low financial capability (e.g. limited knowledge of insurance products)

Step 2: Define the good outcomes

- Example: post sale and post renewal comprehension scores > 85%

Step 3: Measure and compare

Identify an overall comprehension score of 75% but with variances between customer groups.

- Customers with no identified vulnerabilities = 90%
- Customers experiencing bereavement = 85%
- Customers with low financial capability (e.g. low literacy) = 40%

Step 4: Root cause analysis and action

The 40% comprehension score for customers with low financial capability triggers investigation and a redesign of communications using inclusive design principles and offers alternative formats like video explainers.

Principle: Averages can mask poor outcomes. Without processing vulnerability data, firms cannot identify, or act on, the outcome gaps that matter most.

PART 2: **VULNERABILITY DATA REQUIREMENTS**

3.3 Third purpose: to drive product and service improvements

Beyond individual support, vulnerability data provides insights for improving products and services for all customers. The Consumer Duty's Product Governance requires firms to:

- Use outcomes data to review offerings
- Enhance products to make them safer and more inclusive by design
- Identify common friction points or sources of harm
- Proactively protect future customers (who may not disclose vulnerability)

When aggregating data for the purposes of product improvements, firms should protect privacy by:

- Anonymising or pseudonymising data
- Removing individual identifiers
- Report at cohort/group level

Example: life insurance - dyslexia-friendly design

An insurer undertakes analysis for a specific product.

Step 1: Data analysis:
Life insurer analyses target market data and discovers above-average levels of dyslexia among their customers.

Step 2: Product redesign:
Creates dyslexia-friendly format option for all customers.

Step 3: Embed in customer journey:
Makes this format available throughout customer journey, using appropriate communication channels, without requiring the customer to repeatedly disclose their condition.

Result:

- Customers with disclosed dyslexia are more likely to benefit
- Customers who haven't disclosed are also more likely to benefit
- All customers benefit from clearer communication
- Reduced complaints and increased satisfaction across the customer base

Principle: Vulnerability data supports product and service improvements that benefit all customers.

PART 2: **VULNERABILITY DATA REQUIREMENTS**

4 What vulnerability data should be processed?

4.1 Collect data on all customers

According to the FCA's Financial Lives 2022 survey, around 47% of UK adults display at least one characteristic of vulnerability at any given time and all individuals face vulnerabilities throughout their lives.[7]

External databases providing access to financial vulnerability data are available. However, at present, there is no source of vulnerability data on health, life events or capability. The only reliable method to identify vulnerable circumstances comprehensively is direct customer engagement.

In practice

This guide assumes that firms will attempt to obtain vulnerability data on all customers at some point during the customer journey, recognising that firms may not have complete data on all customers immediately. The realistic expectation is that data will be enhanced over time (see Section 5.1).

4.2 Record sufficient information for effective support

Firms may perceive a conflict between two regulatory requirements: UK GDPR's data minimisation principle of 'collect only what you need' and Consumer Duty's requirement to understand vulnerability comprehensively across your customer base and target market.

Data minimisation allows firms to store what they need and for the reason they need it. However, the practical challenge is that firms cannot always predict in advance the following aspects:

- All potential vulnerabilities customers may experience
- Exactly how they will support each type of vulnerability
- Which vulnerabilities will become relevant as customer needs evolve
- How vulnerability data might be used to improve products and services over time
- Future availability of forms of support that firms may add over time

FCA requirements provide legitimate grounds to process customer circumstances that may indicate support needs, even where specific support interventions may not be in place at the time of processing vulnerability data. As explained in Section 3 of Consumer Duty the FCA requires firms to:

- Identify where additional support may be needed
- Understand outcomes for vulnerable customer groups
- Use vulnerability data insights to drive continuous improvement in products and services

7. Financial Conduct Authority, Financial Lives 2022 survey: insights on vulnerability and financial resilience relevant to the rising cost of living (FCA, London 2022)

PART 2: **VULNERABILITY DATA REQUIREMENTS**

Distribution chain considerations. The processing of vulnerability-related data has practical application beyond a single firm, namely:

- Information that one firm cannot immediately use may enable another party in the distribution chain to deliver better customer outcomes
- An intermediary may not know what support capabilities a product provider has developed or will develop
- A product provider may not understand the full context of a customer's circumstances without information gained from the intermediary

Firms therefore should record data that could reasonably enable other firms to support customers with support needs. As expressed in the joint FCA and ICO statement on vulnerability-related data, "under the Consumer Duty, the FCA expects manufacturers (such as lenders and payment networks) and distributors (such as intermediaries and financial advisers) to work collaboratively, sharing relevant information as necessary to deliver good outcomes for consumers".[8]

Good practice

Do record vulnerability information when:

- You have obtained consent or have another lawful basis
- You are clear with customers about what you are collecting and why you're collecting it
- The information relates to your products or services or the support needs of the customer
- It could reasonably help you, or others in the distribution chain, support the customer
- You can store the data securely with appropriate access controls
- You document and update the records of processing activities for any vulnerability data you are processing

Don't avoid recording information simply because:

- You haven't yet developed a specific support process
- You're not certain how other firms will use it
- You don't have all customer support needs in place yet

Guiding principles for intermediaries:

- Collect what is necessary to assess customer needs across your full product range
- Share product-relevant information
- Be transparent to customers, who should understand that you're gathering information to plan appropriate support, regardless of which products are ultimately recommended
- When uncertain, share relevant vulnerability information to avoid potential liability for failing to communicate circumstances that could enable better outcomes

This approach balances comprehensive vulnerability understanding with data minimisation, meeting both Consumer Duty and UK GDPR requirements.

8. Financial Conduct Authority, Joint FCA and ICO statement on regulatory expectations regarding firms' approaches to vulnerability related data (FCA, London 2026)

PART 2: **VULNERABILITY DATA REQUIREMENTS**

5 How should vulnerability data privacy be implemented?

The principles outlined in this section reflect how most firms operate in practice. However, these may not apply to every organisation. Readers should assess their own situation and consult their DPO to determine the most suitable approach for their firm.

5.1 Gradual vulnerability data enhancement

Firms will be at different stages of building a comprehensive understanding about their customer base's vulnerabilities and support needs. This information is typically gathered during product lifecycle touchpoints, including:

Touchpoint	Opportunity
New business sales	Initial vulnerability assessment
Service/product renewals	Review and update circumstances
Claims	Identify vulnerabilities affecting a claim
Complaints	Discover unmet vulnerability needs
Periodic reviews	Scheduled check-ins to update circumstances
Customer-initiated contact	Reactive disclosures
Life events	Proactive contact at known trigger points, e.g. retirement

Given the timing of these interactions, developing a complete picture of customer vulnerabilities is an incremental process that may span several years in order to achieve meaningful coverage across an entire product portfolio.

PART 2: **VULNERABILITY DATA REQUIREMENTS**

5.2 Use proactive and reactive methods to identify vulnerability

The CII recommends that firms employ a hybrid approach to collect customer vulnerability data, combining proactive and reactive methods. The table below describes key features of each approach:

Aspect	Proactive identification	Reactive identification
What are they	Delivered through planned outreach using scheduled reviews, surveys and systematic data analysis.	Triggered by customers' interactions with front-line staff or red-flag events – including voice or text analytics.
How to deploy	**Systematic outreach programmes:** • Vulnerability surveys sent to customer segments • Scheduled review calls based on risk (for example, quarterly or annually) • Life-event monitoring through publicly available records (for example, deaths or change of address) • Financial stress indicators from transactional data analysis **Data analytics approach*:** • Behavioural pattern analysis (for example, spending changes or missed payments) • Demographic profiling for life-stage transitions • Predictive modelling for vulnerability likelihood **Any inferred insights should be verified directly with the customer* **Targeted interventions:** • Automated surveys triggered by severity indicators of life events • Proactive outreach to customers who are approaching retirement • Health and financial resilience questionnaires • Regular check-ins for previously identified vulnerable customers	**Technology solutions:** • Call monitoring software with keyword detection (for example, distress, financial difficulty, health mentions) • Chat analytics for emotional tone and vulnerability indicators • CRM system flags for complaints patterns or service usage spikes • Staff alert systems for immediate escalation **Process implementation:** • Equip front-line staff with customer vulnerability identification skills • Create standardised handover protocols for specialist teams • Implement same-day response procedures for high-severity cases • Establish clear escalation pathways with defined timeframes **Staff training:** • Role-play scenarios for recognising verbal and written distress cues • Active listening techniques for phone and face-to-face interactions • Documentation of requirements for vulnerability indicators • Empathy training and appropriate response protocols
Suitable for	**Optimal for:** • Prevention and early-intervention strategies • Identifying hidden vulnerabilities which customers haven't disclosed • Long-term relationship management and support planning • Understanding emerging vulnerability trends across your customer base • Customers who may not proactively seek help due to pride, stigma or lack of awareness **Best deployed when:** • You have stable, long-term customer relationships • Your products or services have long-term impacts (for example, mortgages, pensions, investments) • You want to build comprehensive vulnerability intelligence	**Optimal for:** • Immediate support needs • Acute vulnerability episodes requiring urgent response • Customers who actively seek help or express distress • Situations where timing is critical (for example, bereavement) • Building staff expertise through real-world experience **Best deployed when:** • You have strong frontline customer interaction • Customers regularly contact your firm • Your products or services have high emotional impact • You need to respond quickly to prevent harm

In practice Proactive identification ensures that all customers are approached to be assessed, while reactive identification is essential for identifying changes.

PART 2: **VULNERABILITY DATA REQUIREMENTS**

5.3 Treat all vulnerability data as special category data

This guide recommends treating all vulnerability-related data as special category data, using explicit consent as the default lawful basis for processing.[9]

The rationale behind this recommendation is that, in practice, most vulnerability information will include special category data at some point. Health conditions, disability information and mental health circumstances are among the most common vulnerabilities experienced by individuals, and all of these constitute special category data requiring enhanced protection under UK GDPR.

The FCA has confirmed that firms need to be proactive in engaging with customers to ascertain their circumstances, including their health status. Hence, even if the person is totally healthy firms should record this 'good health' status, which itself is special category data.

Treating all vulnerability data as special category data is more cautious than legally required in every situation, but it represents the most practical approach for most firms. Attempting to separate special category data from other vulnerability data not categorised as such creates implementation challenges, including:

- Staff need to determine which legal basis applies to each piece of information
- Systems need to handle different data types differently, and as customer circumstances change, firms would need to shift between different lawful bases
- This complexity increases administrative burden, creates system challenges, and exposes firms to greater risk of errors

Consistently treating vulnerability data as special category data delivers the following benefits:

- Customers receive stronger protections
- Systems and processes are simpler to design and operate
- Staff training becomes more straightforward

Important to note:

'Implied health data' is treated as 'health data' and is therefore categorised as special category data.

Examples

What you record	Why it's Special Category Data
"Customer uses sign language"	Implies hearing impairment — health data
"Customer requested wheelchair-accessible venue"	Implies mobility impairment — health data
"Customer mentioned taking antidepressants"	Indicates mental health condition — health data

When this approach may not be optimal

Special category data must be managed under Article 9 of UK GDPR, which imposes stricter requirements than Article 6 (which governs ordinary personal data). In some circumstances, applying special category data standards may be more onerous than necessary.

Bereavement, not considered special category data, provides a clear example. The immediate priority in this scenario is providing sensitive, timely support rather than obtaining explicit consent, which in these circumstances would create unnecessary delays and add distress.

Firms with established bereavement support processes designed around Article 6 requirements (such as legitimate interests) may reasonably continue using those processes without requiring explicit consent.

In practice

Treating all vulnerability data as special category data has implications for the lawful basis for processing. This is covered in Section 6.2.

9. UK GDPR generally prohibits processing special category data unless one of the specific conditions in Article 9 is met. Explicit consent is the most straightforward of these conditions: it gives customers control over their sensitive information and aligns with the trust-building principles that underpin effective vulnerability management. While other Article 9 conditions exist (such as substantial public interest or vital interests), these are typically fallback options for situations where explicit consent cannot be obtained, rather than preferred default approaches.

PART 2: **VULNERABILITY DATA REQUIREMENTS**

5.4 Integrate vulnerability data privacy into existing processes

Many financial services firms will have contracts in place with their customers which include permissions to hold personal data, and in many cases, firms will obtain the customer's permission to store this data as part of the onboarding process under 'explicit consent.'

In practice

If you already obtain explicit consent for processing personal data, extending this to vulnerability data should be relatively simple to adopt.

5.5 Centralise decisions on vulnerability data management

Firms typically determine their data management approach centrally, establishing which data protection principles apply and embedding these decisions within systems, policies and procedures. Individual staff have little leeway to deviate because these decisions require specialist knowledge.

Allowing individual employees to make these determinations case-by-case creates several problems:

- It generates inconsistent decision-making across the organisation as staff may apply different lawful bases for similar situations
- It places unreasonable burden and risk on individual staff members
- It might make compliance unauditable, as there would be no systematic approach to demonstrate

Some cases will require staff to assess what lawful basis to apply, for example when a third party discloses a vulnerability, or in matters of life and death. These are explained in Section 6.3.

Good practice

Core decisions about vulnerability data processing should be policy decisions made at governance level.

The firm's responsibility is to then create clear policies and procedures that staff can follow easily and confidently. Staff should know exactly what to do in standard situations and when to escalate unusual circumstances for specialist guidance.

5.6 Ensure systems are fit for purpose

Effective vulnerability data management requires adequate systems with role-based access controls, comprehensive audit trails, secure backup and recovery capabilities, and integration with operational workflows. Well-designed systems embed data protection practices, control how data is managed, enable compliance and restrict improper use.

The CII's ***Managing customer vulnerability: a practical implementation guide*** includes a systems requirements checklist. Firms are encouraged to assess their current systems against these requirements and invest in appropriate technology to support compliant vulnerability data management.

PART 3: **ESTABLISHING POLICIES**

6 Lawful basis for processing

This is a succinct guide to lawful basis for processing vulnerability data. When determining the lawful basis for processing data in your firm you should consult your firm's DPO.

Data protection laws don't preclude vulnerability information from being processed, as long as:

- There is a regulatory obligation to process the data, or
- The data is necessary for a legitimate purpose, such as supporting customers, and
- The minimum data to achieve this goal is maintained, or
- The customer provides explicit consent to the data being processed

A summary of the most common scenarios and the corresponding Article 6 and Article 9 bases is set out in Appendix 1 (Lawful bases for processing vulnerability data: scenario matrix), which can be used as a quick-reference tool alongside the detailed guidance below.

6.1 Establishing the purpose for processing

The first step in establishing an effective data protection policy relating to customer vulnerability data is to clearly define the purpose for processing such data. Section 3 outlined the three purposes that enable firms to meet both regulatory obligations and a customer's needs.

Why purpose matters

A well-defined purpose is the foundation for all data handling practices because it dictates:

What it determines	How it helps
What data to record	Ensures relevance and minimisation
When to record it	Guides collection timing
How data will be used	Defines processing activities
Why it's legitimate	Establishes lawful basis
How long to retain it	Sets retention periods
How to build/procure systems	Informs technical requirements
How to train staff	Shapes training content
How to communicate with customers	Enables transparent messaging

Good practice

Your purpose for processing statement should:

- Explain the need to record vulnerability data
- Consider customer needs alongside FCA requirements
- Find the balance between what appears to be competing regulations, e.g. UK GDPR data minimisation principle and Consumer Duty Board reporting
- Provide clarity to data processors about why personal data is required

Example purpose statement:

At [company name] we would like to understand your personal circumstances so we can better support you. This includes a reasonable understanding of your health, lifestyle and any additional supports or adjustments you may require. This is also a regulatory requirement by the Financial Conduct Authority. We will maintain your information confidentially. More information is available at [insert website, policy guide, contact number etc.].

PART 3: **ESTABLISHING POLICIES**

6.2 Default lawful basis: explicit consent Article 9(2)(a)

This guide recommends using explicit consent as the primary method for processing vulnerability data. This recommendation assumes that all vulnerability data will be treated as special category data (see Section 5.3).

Characteristics of explicit consent:

- Clear affirmative action: Requires a direct, positive action, such as clicking 'Accept', rather than silence or pre-ticked boxes.
- Informed: The individual must receive clear information about the data controller, purpose, data sharing and their rights before consenting.
- Specific: Consent must be for a defined purpose (e.g. support customer, service improvements etc.) and not be vague or general.
- Voluntary: Must be without coercion, pressure or intimidation.
- Revocable: Users must be able to easily withdraw their consent at any time.

Why explicit consent is preferred for vulnerability data management:

Reason	Explanation
UK GDPR favours it	Assuming all vulnerability data is treated as special category data, other methods can only be used when explicit consent is not feasible
Builds trust	Engenders transparency, customer control and trust
Easy to implement	In most cases, it's straightforward to obtain
Consistency	Likely already used for other product/contract information
Flexibility	Allows data management beyond strict 'necessity'

Good practice

Explicit consent should:

- Be documented (who, when, how, what they were told etc.)
- Include clear explanation of how data will be used
- Allow customers to withdraw consent
- Be reviewed periodically
- Be separate from other purposes (not bundled)

PART 3: **ESTABLISHING POLICIES**

6.3 Alternative lawful bases

There are operational situations where explicit consent under Article 9(2)(a) is unavailable or inappropriate, and firms must instead rely on another Article 9 condition. Common examples include:

- The customer cannot be contacted
- The customer lacks capacity to consent
- Emergency processing is required and consent cannot be obtained in time
- The customer refuses or is unable to provide consent
- A third party discloses the vulnerability

Appendix 1 provides a scenario matrix mapping each common situation to the relevant Article 6 basis and Article 9 condition. The following sections explain which statutory lawful bases firms can rely on when these situations arise.

6.3.1 Legitimate interest - Article 6(1)(f)

Legitimate interest allows firms to process non-special category data for reasonable business purposes without relying on explicit consent, provided it doesn't override the individual's fundamental rights and interests, e.g. sending third-party marketing and communications.

Limitation: Special category data cannot rely on Article 6 alone, it requires:

1. Article 6 basis (such as legitimate interest) AND
2. Article 9 condition (such as explicit consent OR substantial public interest)

Example

Scenario: Processing customer's contact preferences (non-special category data)

Can use: Legitimate interest Article 6(1)(f)

Scenario: Processing customer's mobility impairment (special category data)

Must have: Legitimate interest Article 6(1)(f) PLUS Article 9 condition (e.g., explicit consent Article 9(2)(a) OR substantial public interest Article 9(2)(g))

6.3.2 Vital interest - Article 9(2)(c)

Vital interest Article 9(2)(c) allows processing special category data, if necessary, to protect someone's vital interests when they cannot consent. This condition applies when processing is essential for safeguarding an individual's life. This may include:

- Emergency medical care
- Potential suicide or self-harm
- Protection from domestic or economic abuse
- Customer unavailable due to physical/mental illness

Limitation: It can ONLY be used if another lawful basis is not available AND the customer cannot consent. If the customer refuses to give consent and is of sound mind, then the data cannot be processed under 'vital interest.'

Example

Scenario: Customer's family calls concerned about an immediate suicide attempt. Customer is unresponsive AND their life is at risk.

Can use vital interest when:

- Situations of life and death AND
- Individual is physically or legally incapable of giving consent

Good practice

When relying on vital interest in emergency situations:

Step 1: Record the immediate concern and take necessary protective action, coordinating with emergency services where appropriate.

Step 2: Once the immediate risk has passed and the customer is able to engage, seek explicit consent retrospectively (if possible). If consent cannot be obtained, transition to an alternative lawful basis such as safeguarding or regulatory requirements.

Document all decisions clearly, including why vital interest was necessary, what actions were taken, and how the lawful basis was managed following the emergency. This ensures both that urgent support is provided without delay and that ongoing data processing remains compliant.

PART 3: **ESTABLISHING POLICIES**

6.3.3 Legal Claims and Judicial Acts - Article 9(2)(f)

Article 9(2)(f) provides conditions for processing special category data where it is necessary for legal claims or judicial acts. This may include processing vulnerability-related data for:

- Present legal proceedings
- Prospective legal proceedings
- Defending legal rights
- Insurance claims
- Complaints that may become legal claims

Limitation: The data retained must be necessary for the potential legal issue, proportionate to the claim and relevant to the legal matter. Article 9(2)(f) is unlikely to cover all vulnerability data typically collected.

Example

Scenario: A customer issues a court claim alleging discrimination due to a mental health condition.

The **legal claim basis can be used to** retain data about the mental health condition, document the complaint and gather evidence for the defence.

It cannot be used to record unrelated vulnerability information and retain data indefinitely beyond claim resolution.

Use special category data for legal claims and judicial acts for an active claim when necessary.

6.3.4 Substantial Public Interest - Article 9(2)(g)

Article 9(2)(g) allows firms to process special category data without consent when doing so is:

"...necessary for reasons of substantial public interest, based on Domestic Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."[10]

There are 23 conditions specified (Schedule 1 Part 2 of the DPA 2018) that qualify as substantial public interest for special category data.[11] The relevant categories for vulnerability data management in financial services are examined in the following sections.

Reliance on any Schedule 1 Part 2 condition requires an Appropriate Policy Document (APD) to be in place at the time of processing.

6.3.4.1 Safeguarding of children and of individuals at risk (Condition 18)

This condition permits the processing of special category data without consent where it is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm; and where the individual is aged under 18, or 18 and over and 'at risk' within the statutory definition.

An adult is considered "at risk" where the controller has reasonable cause to suspect that the individual (a) has needs for care and support, (b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and (c) as a result of those needs is unable to protect themselves against the neglect or harm or the risk of it. All three limbs must be present.

Limitation: Special category data can be processed without consent when:

- The individual cannot give consent in the circumstances
- The controller cannot reasonably be expected to obtain consent
- Obtaining consent would prejudice the provision of the protection

10. Information Commissioner's Office, 'What are the conditions for processing?', UK GDPR Guidance and Resources, (ICO, London 2023)
11. 'Data Protection Act 2018 (c. 12), Schedule 1, Part 2', Legislation.gov.uk (Crown Services, London 2018)

PART 3: **ESTABLISHING POLICIES**

Example: Suspected domestic abuse disclosed during a call

Scenario: A customer calling to discuss a joint policy becomes distressed and indicates that a co-policyholder is controlling their finances and blocking access to shared accounts. They indicate they cannot safely discuss it further.
The indicators meet the "at risk" definition: needs for support, risk of emotional or physical harm, inability to protect themselves. Obtaining formal consent to record the disclosure and flag the account could prejudice the protection if it reaches the co-policyholder.

✔ **The firm may rely on Condition 18 to:**

- Record the disclosure and the indicators of risk
- Apply appropriate account protections, e.g. suppressed communications, separate contact channel
- Share data with and coordinate with internal specialist teams or appropriate external services

Follow-up:

- Inform the customer of what has been recorded once it is safe to do so
- Document the rationale, including the 'at risk' indicators, why consent could not be sought, the protective purpose, and the substantial public interest justification

6.3.4.2 Safeguarding economic well-being of certain individuals (Condition 19)

This condition permits the processing of special category data without consent where it is necessary to protect the economic well-being of an "individual at economic risk" , defined as an adult (18+) who is less able to protect their economic well-being because of physical or mental injury, illness or disability.

⚠ **Limitation:** special category data can be processed without consent when:

- The individual cannot give consent in the circumstances
- The firm cannot reasonably be expected to obtain consent
- Obtaining consent would prejudice the provision of the protection

Example: Customer in acute distress during a call

Scenario: A customer shows signs of severe mental distress during a call and is about to make an irreversible financial decision (e.g. liquidating a pension, transferring funds to a third party). Pausing to seek explicit consent to record the distress and act on it would prejudice the firm's ability to protect them from immediate economic harm.

✔ **The firm can rely on Condition 19 to:**

- Record the indicators of distress insofar as they bear on economic risk
- Pause or delay the transaction and implement appropriate support measures
- Coordinate with relevant internal teams or external services

Follow-up:

- Inform the customer of what has been recorded once it is appropriate to do so
- Seek consent retrospectively, where possible, and adopt a straightforward basis thereafter
- Document the rationale for relying on the safeguarding basis, the specific economic risk identified, and why consent could not be obtained at the time

PART 3: **ESTABLISHING POLICIES**

6.3.4.3 Insurance (Condition 20)

This condition permits the processing of specified categories of special category data without consent where it is necessary for an insurance purpose. Insurance purpose is defined as:

- Advising on, arranging, underwriting or administering an insurance contract
- Administering a claim under an insurance contract
- Exercising a right, or complying with an obligation, arising in connection with an insurance contract (including rights and obligations arising under an enactment or rule of law)

Applies to insurers, reinsurers, insurance intermediaries and brokers, and others carrying out the functions above.

Example: Underwriting a life insurance policy

Scenario: A customer applies for a life insurance policy. As part of the application, the insurer asks about her medical history. She discloses she is being treated for high blood pressure and was diagnosed with breast cancer four years ago (now in remission).

The firm relies on Condition 20 (rather than explicit consent under 9(2)(a)), because:

- The health data is necessary to underwrite the contract
- Consent that is required as a condition of obtaining the service is not "freely given" under UK GDPR and would not be a valid basis

The firm should:

- Use the data solely for the insurance purpose
- Issue a privacy notice explaining how the data will be used

Good practice

Document your lawful basis

Whichever rationale for processing is used, **this must be documented**.

Standard approach:

- Use explicit consent as default
- Document when consent is obtained
- Record only alternative lawful bases when used (by exception)

Documentation of alternative purposes should include:

- Which lawful basis used
- Why it was chosen
- When decision was made
- Who made decision
- Review date

PART 3: **ESTABLISHING POLICIES**

7 Embedding vulnerability into data protection policies

7.1 Integration with existing policies

Vulnerability-related data should be explicitly addressed within your core data protection documentation, including your Record of Processing Activities (ROPA), data retention schedules, data sharing agreements, and incident response procedures. This integration ensures that vulnerability data receives appropriate treatment within established processes rather than being managed as an isolated exception.

Where vulnerability data requires specific procedures due to its sensitivity, e.g. enhanced access controls, specialised staff training or consent mechanisms, these should be documented as addenda or specific sections within your broader policies rather than as standalone documents.

7.2 Documenting how vulnerability data is processed

The accountability principle in UK GDPR requires firms to demonstrate compliance. Organisations must maintain clear records documenting how vulnerability data is processed. Examples follow.

What to record	Why	Where to document
Purpose for processing	Why vulnerable customer data is collected (e.g. to ensure appropriate customer support)	Data processing policy, privacy notices
Lawful basis	Which Article 6 basis and Article 9 basis and UK DPA 2018 Schedule 1 condition (if applicable). Appendix 1 sets out the typical combinations for common scenarios.	Data processing policy, Record of Processing Activities (ROPA)
Appropriate policy document	Required for special category data under UK law (i.e. internal policy outlining how you handle and protect data)	Data protection policy, vulnerability data handling procedure

Good practice

Ensure your documentation includes:

- Data Processing Impact Assessment (DPIA) for vulnerability data
- Vulnerability Data Handling Policy
- Staff procedures and training materials
- Privacy notices explaining vulnerability data use
- Regular audit and review records

7.3 Privacy notices

Transparency extends beyond internal documentation, to customer communications. Privacy notices must inform customers that you may collect vulnerability information, enabling them to make informed decisions about disclosures.

Your privacy notice should clearly explain:

- That you collect vulnerability information
- Why you collect it (the purpose)
- How you'll use it
- Who you might share it with
- How long you'll keep it
- Their rights (e.g. access, correction, deletion etc.)

Example privacy notice extract

We collect information about your circumstances that may affect how we support you. This might include health conditions, life events, or financial circumstances that mean you need non-standard or additional support.

We use this information to provide you with appropriate support, ensure our products and services work well for you, and to meet our regulatory obligations.

We'll only share this information with others in our organisation who need it to support you; and with carefully selected partners where this helps us provide better services. You can ask us to delete this information at any time.

PART 4: **OPERATIONAL DATA MANAGEMENT**

8 Managing vulnerability data in practice

This section covers day-to-day data management; how to compliantly collect, record, maintain, store and share vulnerability data; as well as how to respond to customer requests about vulnerability data.

8.1 Collect vulnerability data

Firms can gather vulnerability information by engaging with customers directly or by using indirect data sources. Before collecting or processing any vulnerability information or data, firms must ensure that appropriate data protection documentation is in place. Given the 'special category' nature of vulnerability data a Data Protection Impact Assessment (DPIA) must be completed prior to initiating any processing activity.

Firms must also keep and update their Record of Processing Activities (ROPA) to reflect vulnerability data processing, documenting the lawful basis for processing, data categories, retention periods, and any third-part sharing arrangements.

8.1.1 Direct data collection (customer-led)

This can be done by engaging directly with customers (either proactively or reactively, see Section 5.2) through questionnaires, scripted calls, online self-disclosures and front-line observations. This approach is subject to customers disclosing their circumstances and requires suitable systems to record, and act, where vulnerabilities are identified.

8.1.2 Indirect data collection

Vulnerability may be inferred through socioeconomic or behavioural data or system-generated triggers.

Common indicators

Category	Examples
Transaction anomalies	• Unusual internal account transfers • Erratic transaction patterns • Sudden changes in financial behaviour
High-risk spending	• Elevated gambling expenditure • Payday loan usage • Potentially harmful financial services
Financial distress	• Increasing debt levels • Payment arrears • Declining account balances
Missed obligations	• Patterns of missed payments • Difficulty managing commitments
Socioeconomic indicators	• Lives in social housing • Area with low mean income • High unemployment area

Limitation: socioeconomic indicators suggest potential vulnerability but do not provide definitive evidence and may be false positives. Under UK GDPR, firms should not record assumptions based solely on socioeconomic proxies as factual vulnerability data. Such inferences may fail data accuracy requirements unless verified through direct contact with the customer.

PART 4: **OPERATIONAL DATA MANAGEMENT**

8.2 Record vulnerability data

Data must be recorded in a consistent, structured format so it is understandable by other users, can be collated and reported on, and supports monitoring outcomes. Recorded vulnerability data should include information about:

- The circumstances
- The severity of the circumstances
- The firm activities
- The potential harm
- The support need
- If the support need was implemented or not
- Review date

Recording free-format notes in text boxes is highly unlikely to meet the above criteria and hence not suitable for meeting Consumer Duty.

8.2.1 Recording inferred data

Section 8.1.2 covered indirect methods, such as using socioeconomic or behavioural data from which vulnerability can be inferred. Firms should record this data indicating an 'inferred status' and verify with the customer the information before recording its status as factual.

Inferred data can also be obtained manually, and if so, should be recorded as inferred data, or ideally the data is clarified during the conversation, so it is factual and not inferred or subject to bias.

Examples: appropriate versus inappropriate manual recording

Inappropriate	Appropriate
"Customer keeps calling, they must have cognitive issues"	Customer called 8 times in 2 days regarding same account query. Call notes show customer required repeated explanations of same basic account features. Date: [X].'
"Customer is probably depressed"	'Customer exhibited low mood during call, mentioned difficulty sleeping and loss of motivation. Date: [X].'
"Customer gambles too much"	'Open banking data shows £500+ monthly gambling expenditure, 40% increase from previous 6 months. Date: [X].'

8.2.1.1 Recording obvious vulnerabilities from inferred data

Where a customer is obviously vulnerable based on inferred data (e.g. spending at a health institution), combined with behaviour consistent with the illness, AND the customer cannot be contacted to consent to the recording of such information, it is UK GDPR compliant to record the data where:

- Information relates to health, AND
- The customer is at risk of economic harm, AND
- The customer is unable to consent OR obtaining consent would be unreasonable OR would prejudice the support the data controller is aiming to provide

As per the Article 9 lawful basis detailed in Section 6.3.4.

8.2.1.2 Exceptions to verification requirements

Direct customer contact may not be appropriate in certain circumstances.

Circumstance	Description	Example
Immediate risk situations	• Customer obviously in severe distress • Delay in support could cause significant harm • Urgent intervention required	Customer on phone expressing suicidal thoughts
Communication barriers	• Customer unable to communicate effectively • Previous contact attempts unsuccessful despite reasonable efforts • Condition prevents meaningful conversation	Customer with severe dementia; family member provides information
Safeguarding concerns	• Contact might expose customer to additional risk/harm • Third-party involvement suspected (e.g. financial abuse, coercive control etc.) • Verification could prejudice safeguarding	Suspected financial abuse by family member who monitors all communications

As detailed in Section 6.3.4, where consent is not appropriate, other lawful bases rather than explicit consent can be used.

PART 4: **OPERATIONAL DATA MANAGEMENT**

8.2.2 Record the right amount of information

The data minimisation principle requires that personal data is adequate, relevant and limited to what is necessary for the purpose for which it is processed. In practice, this means recording only what is needed, no more. This section provides examples of the types of data that can be recorded.

Data recording table

Data element	When it can be recorded	Reason	Considerations
Consumer circumstances (e.g. depression, cancer, job loss, bereavement etc.)	Where circumstances may fluctuate Where circumstances may return in the future Where circumstances, identified through support, need disclosure	To provide vital contextual information for other members of the team or other firms To ascertain the appropriate support for the customer, especially as some conditions are fluctuating by their nature To prevent the need to continually redisclose the circumstances: an FCA expectation	Customers should be aware of the processing of their data, why and how it will be used System fields: Dropdown categories + severity rating + free text only for specifics
Duration of circumstances (How long affecting customer)	All cases	Understanding the bigger picture enables appropriate support decisions and supports Consumer Duty compliance by avoiding foreseeable harms	Appropriate to know whether the vulnerability has been impacting the customer for a long time and in cases of new vulnerabilities System field: Date first identified + duration estimate
Previous occurrences (Whether circumstances previously active)	All cases	Understanding the bigger picture enables appropriate support decisions, supports Consumer Duty compliance through avoiding foreseeable harms	Appropriate to know whether the vulnerability has been impacting the customer for a long time and in cases of new vulnerabilities Example system field: Checkbox 'Previous episodes' + dates
Support needs (What support is required)	All cases	Record not only what the circumstance is but what the customer is vulnerable to, and why the support is fundamental to supporting the customer	Data needs to be maintained throughout customer relationship unless it's declared no longer relevant Example system field: Structured support needs categories are linked to firm activities
Product/service adjustments (Subset of support needs)	Where the risk of the vulnerability can be mitigated through product or service designs	Whilst this is a subset of support needs, it's justified to have its own category as required for Consumer Duty (e.g. outcomes monitoring plus future product reviews and approvals)	Detailed data may be kept on customer account For governance purposes (e.g. outcomes monitoring, product reviews, board reports etc.) remove customer details (i.e. aggregate/anonymise) Example system field: Link to product adjustment catalogue
Root cause of vulnerability	All cases (where identifiable)	The presenting vulnerability may not be true cause. The FCA encourages tackling root cause	Only where root cause can be accurately identified. It's important to include only factual information System field: Separate from 'presenting circumstance'

PART 4: **OPERATIONAL DATA MANAGEMENT**

Data recording table continued

Data element	When it can be recorded	Reason	Considerations
Third party authority data	Where authorised third party allocated (including power of attorney)	Personal details of the third party are required to maintain confidentiality in future interactions, whilst complying with requirements not to circumvent authorised third parties	Obtain consent from third party to maintain their data Example system fields: Third party name, relationship, contact details, authority type, verification date
Customer opinions	Where customer gives opinions about condition or support needs	Reasonable expectation to record opinions relating to support required	Record customer views, not staff opinions Example system field: Free text clearly labelled 'customer feedback'

Example: Mental health condition recording

Circumstance category:
[Health] > [Mental Health]

Specific condition:
[Depression]

Severity:
[Moderate]

Fluctuation:
[Yes - episodes typically last 3-6 months]

Vulnerable to:
- ☑ Making rash financial decisions
- ☑ Missing important communications
- ❑ Understanding complex information

Support needs:
- ☑ Regular proactive check-ins (monthly)
- ☑ Payment flexibility during episodes
- ☑ Simplified communication
- ❑ Third party involvement

Root cause:
[debt stress]

Customer's feedback:
"I'm usually fine between episodes but when it hits, I can't cope with paperwork at all"

PART 4: **OPERATIONAL DATA MANAGEMENT**

8.3 Keeping data accurate

8.3.1 Why data accuracy matters

Article 5(1)(d) UK GDPR mandates that data accuracy needs to be correct and up to date because outdated or wrong data may lead to inappropriate support or deny the customer suitable help. There are two dimensions to maintaining accuracy:

1. Accurate when recorded (covered in Section 8.3.2 of this guide)
2. Kept up to date (covered in Section 8.3.3 of this guide)

In the context of vulnerability data management, accuracy matters because:

- Circumstances change or are resolved
- New vulnerable circumstances emerge
- Severity or support needs may change over time
- Customer learns to manage condition

Data decay: non-vulnerability context

Accurate vulnerability-related data often exists within broader customer contact data. It is estimated that contact data decays at a rate of circa 10-15% per annum due to people moving house, changing email, deaths, relationship changes etc.

Implication: Regular data hygiene reviews are essential for all customers, because a customer can become vulnerable at any time, and vulnerability assessment can only be accurate when changes in data and circumstances are accurately noted.

8.3.2 Ensuring data accuracy at the point of recording

The ICO recognises that it is impractical to corroborate every piece of information provided. Instead, they recommend the following steps when recording personal information provided by a customer or third party.

Recommended steps when recording personal information:

Step	What to do
Record data objectively	Record information in customer's or third party's exact words (if verbal) or actual responses (if digital)
Record source	Note details of disclosing individual
Take reasonable steps	If verbal, repeat information back. If digital, confirm back to the consumer; or if other data sources are available cross check
Consider challenges	Carefully consider any customer disputes as to accuracy

8.3.2.1 Recording comments

When verbal interactions occur, a poorly worded comment can mislead colleagues handling a future interaction, prejudice the customer's outcomes, and create a record the firm would struggle to defend in a subject access request or regulatory review. The tables below give examples of the types of comment that can safely be recorded, and those that should not.

Safe to record

Type of comment	Examples
Factual observations	'Customer was distressed' 'Customer unable to understand information being provided' 'Customer appeared irritated'
Customer's own comments	'Customer said: "I struggle with written documents due to my dyslexia"' 'Customer stated they feel overwhelmed by financial decisions since bereavement'
Objective descriptions	'Customer called 8 times in 2 days about same issue' 'Customer requested large print documents'

PART 4: **OPERATIONAL DATA MANAGEMENT**

Comments not suitable to be recorded:

Type	Why	Example
Staff opinions inferring vulnerability	Subjective, potentially harmful	"I think customer has dementia"
Assumed diagnoses	Not verified, potentially incorrect	"Customer is clearly depressed"
Health information where customer unaware	May cause harm without health professional assessment	"System flagged for potential cognitive impairment based on call patterns" (unless corroborated by professional health)
Judgmental comments	Unprofessional, potentially harmful	"Customer is being difficult" "Customer is overreacting"

Good practice

Recording comments manually

Principles for recording comments
- Must be objective
- Must be factual
- Must be accurate
- Must be something you can disclose to the customer

Do record:
- What the customer said/did
- Objective observations
- Actions taken

Don't record:
- Staff assumptions
- Diagnoses staff are not qualified to make
- Judgments about the customer's character/behaviour

Structured digital solutions rather than human free form text, minimise subjective assessments and human error and UK GDPR liability.

8.3.2.2 What about emails or other similar data?

The same principles outlined in Section 8.3.2.1 apply to digital communications. Digital communications between the firm and customer are also considered personal information.

Example: Email comments

Professional email (safe to record): "Customer mentioned during call that they have anxiety which sometimes makes phone conversations difficult. Have noted on account and offered email communication as alternative."

Unprofessional email (problematic to record): "This customer was really anxious on the phone. Probably has some mental health issues. They kept asking the same questions."

Better alternative: "Customer requested information be repeated several times and expressed preference for email communication. Updated communication preference on account."

8.3.2.3 What about flags or system codes?

Flags and system codes are personal information and the principles outlined in the previous sections also apply.

Examples:

Data fields	Record?	Why/why not
'VUL-MH' (Mental health vulnerability)	Yes	Factual, verified
'NEEDS-SUPPORT'	Yes	Objective, actionable
'PROB-COG' (Probable cognitive impairment)	No	Unverified assumption
'DIFFICULT-CUST' (Difficult customer)	No	Judgmental, not vulnerability-related

PART 4: **OPERATIONAL DATA MANAGEMENT**

8.3.3 Keeping data up to date

Article 5 requires firms to take "every reasonable step" to rectify inaccurate data without delay. This includes considering whether periodic updates are necessary.

When to review vulnerability data:

Vulnerability state	Review frequency	Example
Unlikely to change	No formal requirement	Stable conditions (e.g. permanent disability)
May fluctuate	Regular reviews needed	Conditions that improve/worsen (e.g., mental health, financial situation etc.)
Temporary	Review at expected resolution	Job loss, bereavement, temporary illness etc.
Support needs may change	Review when support needs implemented	If a new support need is introduced by the firm, cross check existing customers in case the support is applicable

The review period will depend on the product/service in question and the circumstances. For example, a customer with debt issues may be appropriate to review monthly or quarterly, while for a fixed-term investment it may be appropriate to review every few years.

Review triggers:

	Proactive	Reactive
Typical existing touchpoints	Policy renewals Annual reviews	Claims Complaints Customer initiated change of circumstances
Specific triggers	Scheduled review dates	Change in circumstances via data feeds Change in transactions Missed payments

8.3.4 Historical records

Customer circumstances are not static. Just because customer data needs to change does not mean the historical data is incorrect or needs to be removed. Historical records should be kept, even when data is updated. This enables the following:

- Evidence of support provided (as required by Consumer Duty)
- Pattern identification (fluctuating conditions)
- Regulatory audit trail
- Reinstating support if the condition recurs
- Defence against complaints

Example: Depression episode resolved

Original recording (March 2024):

Circumstance: Depression (moderate severity)

Support need: Monthly check-ins, payment flexibility

Status: ACTIVE

Recorded by: Agent J. Smith, 15/03/2024

Source: Customer disclosure

Update after review (September 2024):

[NEW RECORD]

Circumstance: Depression

Severity: No longer active

Support need: None currently required

Status: RESOLVED

Updated by: Specialist M. Brown, 20/09/2024

Source: Customer review call

Review date: 20/03/2025 (6-month check)

[HISTORICAL RECORD - DO NOT DELETE]

Circumstance: Depression (moderate severity)

Support need: Monthly check-ins, payment flexibility

Status: HISTORICAL (was active Mar-Sep 2024)

Original recording: Agent J. Smith, 15/03/2024

PART 4: **OPERATIONAL DATA MANAGEMENT**

Good practice

Systems should:

- Keep accurate records of previous data
- Maintain appropriate metadata (including who provided this and when)
- Clearly distinguish between current and historical data/records
- Preserve audit trail

8.3.4.1 Incorrectly recorded information

It is acceptable to keep a record of mistakes, including noting vulnerabilities which should not have been noted. However, such records must be recorded in a way to make it clear a mistake was made.

Example:

[RECORD MARKED: RECORDED IN ERROR]

Date recorded: 15/03/2024

Circumstance incorrectly recorded: Diabetes

Reason: Wrong customer account

Corrected by: Supervisor T. Wilson, 16/03/2024

Action: Moved to correct customer account #67890

8.3.4.2 How to manage historical data

Historical data can be retained but must be suitably marked, so only the current data is used. If data is found to be incorrect, it should be marked as such.

Action	When to action	Example
Update	Vulnerabilities/ conditions develop	Depression becomes more severe: update severity rating
Reclassify	Condition changes into different condition	Anxiety disorder diagnosed as bipolar: reclassify main condition
Remove from live record	Customer no longer vulnerable	Record status and retain historical record
Keep	Always for audit/ compliance	All historical records of data, support provided, and changes made
Mark as incorrect	Data recorded incorrectly	Record as error, explain correction, preserve for audit purposes
Delete entirely	Customer exercises right to erasure	Delete/anonymise from live systems, manage in backups

Good practice

Metadata should be recorded for all changes:

- Date of change
- Who made change
- What changed (before/after)
- Why changed
- Source of information

This data enables:

- Clear audit trail
- Current data easily identified
- Historical pattern analysis
- Regulatory compliance evidence

PART 4: **OPERATIONAL DATA MANAGEMENT**

8.4 Retention

As a starting point, vulnerability data should not be kept for longer than necessary, i.e. it should generally be retained for the same period as the product or service being provided, or which it relates to.

Different retention rules for different data states

Data state	Retention approach
Live vulnerability data	While product is active plus a reasonable period after, aligned with the product retention policy. It supports continuous delivery of customer support
Historical vulnerability data	Retained for audit/compliance purposes, with the dates it was recorded. This supports outcome reporting
Incorrect data	Retained (recorded as incorrect) for audit trail

Vulnerability data may be retained after the general retention rule

- After vulnerability no longer impacts the customer, it must be reclassified as inactive data or as a historical record
- In multiple system locations (but must be applied consistently)
- For regulatory/compliance purposes beyond immediate customer support need: it must be clearly identified by data and the status of any support need

8.5 Storing vulnerability data safely

UK GDPR's security principle (Article 5(1)(f)) mandates appropriate security to protect confidentiality and integrity. It applies equally to in-house servers and cloud storage. The following measures can help ensure compliance:

Practice	What to implement	Why it matters
Know where data is	• Maintain inventory of all systems storing vulnerability data • Identify: core systems, call recordings, emails, case management etc. • Maintain data maps	Vulnerability data may be scattered across systems. Good practice: restrict to 1 or few systems for proper management
Access controls	• Implement role-based access control (RBAC) • Only enable access on a need-to-know basis • Implement tiered access	Limits who sees or uses sensitive data, e.g. specialists see full details, others see flags only
Physical and network security	• Apply best practice standards for security, e.g. ISO 27001, cyber security essentials	Protects from external threats and unauthorised physical access
Use reputable services	• Providers with ISO 27001 or similar certification • Contract requires them to protect data • Regular security audits	UK GDPR requires cloud processors give sufficient security guarantees
Back up data	• Regular automated backups • Encrypted backup storage • Separate storage • Test restore procedures	Ensures recovery from data loss/cyber attack without exposing data

PART 4: **OPERATIONAL DATA MANAGEMENT**

8.6 Responding to customer requests regarding vulnerability data

8.6.1 Right to erasure (the right to be forgotten)

This section focuses on requests to delete vulnerability information, not complete customer records. The key question here is when does right to erasure apply and what is the basis to carry this out.

8.6.1.1 Where the lawful basis is consent

Where the lawful basis for processing the data is consent or explicit consent, the customer retains the right to erasure which the firm cannot override.

Example:

Customer gave explicit consent to record anxiety condition and later requests this record is deleted.

Firm must:

- Delete the vulnerability data and record
- Confirm deletion to customer within 30 days
- Remove/anonymise vulnerability data from all systems (including backups)

It is advisable to inform the customer that once vulnerability data is deleted; the firm won't be aware of the support or adjustments they need (if already recorded).

8.6.1.2 Where the basis is legitimate interests

If processed under legitimate interest Article 6(1)(f), see Section 6.3.1, the customer has no blanket right to erasure, instead the controller must assess whether there is an overriding legitimate interest to continue to process the data.

Example:

Firm A records vulnerability following a customer email disclosing a medical condition requiring support. Unable to reach customer, they use legitimate interest paired with economic wellbeing to record the information. In line with the transparency principle they notify the customer, who later requests deletion of their medical condition.

Assessment Firm A does NOT have to automatically comply but should assess whether it's in the customer's best interests for support to continue (and therefore data to be retained).

It is advisable to inform the customer that once vulnerability data is deleted, the firm won't be aware of the support or adjustments they need (if already recorded).

PART 4: **OPERATIONAL DATA MANAGEMENT**

It is appropriate to retain records/data in certain circumstances including:

Situation	Why retention justified
Dementia or memory-affecting condition	Customer may not recall need for support and deletion could cause harm
Bipolar disorder with known episodes	Likely to experience future episodes requiring resumed support
Condition impairing decision-making	Customer may lack capacity to make an informed deletion request
Recent severe episode	Request may be made during crisis and retention protects from harm

8.6.1.3 Other circumstances where right to erasure applies

The right to erasure does not rest solely on the customer's wishes. UK GDPR Article 17 sets out a defined list of circumstances in which erasure is required, regardless of whether the customer has asked for their data to be deleted. The table below summarises each circumstance and what it means for vulnerability data.

Circumstance	Explanation	Implication for vulnerability data
Purpose no longer applies	The data is no longer necessary in relation to the purposes for which it was collected or processed	Where the purpose includes maintaining evidence of regulatory compliance (e.g. under Consumer Duty), processing may legitimately continue for a reasonable period after support has ended
Data processed unlawfully	The data has been unlawfully processed either because no valid lawful basis existed or because the original basis has expired and no replacement applies	Vulnerability data recorded without a valid lawful basis, or where the basis no longer holds, must be deleted
Legal obligation to erase	Erasure is required to comply with a legal obligation in UK laws	Rarely applicable to vulnerability data in practice
Direct marketing	Data was processed for direct marketing purposes	Not applicable in the context of vulnerability data

8.6.1.4 Deleting data from back-up systems

The ICO says "if a valid erasure request is received and no exemption applies then you will have to take steps to ensure erasure from backup systems as well as live systems."

However, they do accept that data may remain in back-up systems for a period until technically possible to delete; this is deemed as acceptable if the data subject is notified accordingly.

ICO guidance

"The key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten. You must ensure that you do not use the data within the backup for any other purpose, i.e. that the backup is simply held on your systems until it is replaced in line with an established schedule. Provided this is the case it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will be context specific."[12]

8.6.2 Data Subject Access Requests (DSAR)

Vulnerability data, like any other personal data, must be in a format that can be provided to the customer under DSAR. Therefore, it should be objective, consistent and devoid of subjective staff assessments. Record the circumstances, severity, and support needed, without making judgments or opinions about the subject.

This guidance is not intended to cover the general rules in relation to the handling of a DSAR, instead it focuses on the interaction between vulnerability and DSARs.

8.6.2.1 Do we include opinions/comments made by staff in responses?

As a rule, any information requested by a customer, that is recorded by the firm and is reasonably available, should be included in responses.

Exceptions:

- Data relating to another data subject (may need to redacted)
- Data subject to legal professional privilege
- Data that would cause serious harm to the physical/mental health of the customer or third party upon disclosure

12. Information Commissioner's Office, 'Right to erasure', UK GDPR Guidance and Resources (ICO, London 2023)

PART 4: **OPERATIONAL DATA MANAGEMENT**

8.6.2.2 How to manage large or complex requests by a data subject

Where a request covers a large volume of data, the ICO guidance provides for the following:

"If you process a large amount of information about an individual, you may be able to ask them to specify the information or processing activities their request relates to, if it is not clear. The time limit for responding to the request is paused until you receive clarification, although you should supply any of the supplementary information you can do within one month."[13]

8.6.2.3 What is a "large amount" of information?

UK GDPR does not specifically define this in quantitative terms. When determining whether the data meets this definition firms should consider:

- Type and sensitivity of data (more effort is expected for sensitive data)
- Frequency of processing
- Extent and scope of processing
- Overall cost and time required to respond

For vulnerability data, given its high sensitivity, it is reasonable to:

- Request clarification of what vulnerability information they want
- Provide options, e.g. 'Do you want support records only, all vulnerability assessments, or complete records?'
- Ensure you still provide core vulnerability information within one month

8.6.2.4 What about where the customer is not aware they have been classified as vulnerable?

While categorising consumers as vulnerable or not may be useful for firm level reporting, it is not recommended for individual categorisations. Firstly, this is too simplistic, and they should record their circumstances and the severity of the circumstances.

Secondly, vulnerability is contextual. People are not always inherently vulnerable, and vulnerability depends on the interaction with the firm. By example, a customer with a gambling addiction faces less potential harm when buying life insurance cover, than when offered high-risk investments or instant credit.

It is appropriate to inform the customer of the source of information, which may be:

- Previous disclosure(s) from the customer they may have forgotten
- Vulnerability databases they may have subscribed with
- Other firms in the distribution chain
- Inferred data, e.g. transactional anomalies, change of address registers, death notifications.

Disclosing health data to the customer may be harmful to them. Adopt the following approach to determine if and how to disclose this data.

- Must not disclose unless a health professional's opinion is obtained [14]
- Professional's opinion must be within last 6 months
- Professional's opinion must confirm that no serious harm to the customer will result from the disclosure

13. Information Commissioner's Office, 'A guide to subject access', UK GDPR Guidance and Resources (ICO, London 2023)
14. Relevant health professionals include registered medical practitioners, dentists and nurses. The DPA provides a full list of the types of professionals that fall within the definition (see Section 204 of the DPA 2018).

PART 4: **OPERATIONAL DATA MANAGEMENT**

9 Sharing vulnerability data

9.1 Tiered access model

Data minimisation requires the data to be only used and seen by those who need to see it. A tiered system for recording and sharing vulnerability information enables firms to process comprehensive vulnerability data while complying with this principle, like how credit scoring provides an actionable rating without disclosing the underlying financial detail. The table below shows a practical example of implementing a tiered system:

Level	Detail provided	Example	Who accesses
1	Vulnerable or not	Yes/No flag	All staff; no limits
2	Support need (action-oriented)	'Ensure family member/carer present'	Anyone who may encounter customer
3	Vulnerability scale	'Very vulnerable'	Most staff who encounter or influence customers
4	Topic level	'Health' (Health/Financial/Life Events/Capability)	Staff who encounter customer but don't prescribe actions
5	More detail on circumstances	'Severe mental health'	Staff who prescribe actions for customer
6	Full detail	'Severe bipolar. On medication. Fluctuating - review every 3 months. Vulnerable to: impulsive decisions during manic episodes. Support: Monthly check-ins, pause major decisions during episodes, involve named family member'	Only staff directly involved in prescribing service for individual

In practice **Small versus large firms**

Large firms may use all 6 levels, while smaller firms may consolidate levels that are less granular, while still restricting access to full vulnerability information. Both large and small firms require a tiered access when sharing with third parties across the distribution chain.

PART 4: **OPERATIONAL DATA MANAGEMENT**

9.2 Sharing within firm

The golden rule when sharing data internally is to do so using need-to-know and role-based-access bases. The following table outlines internal sharing best practices.

What to do	Why	How
Tell the customer up-front	Meets transparency principle. Encourages honest disclosure	At the point of disclosure, communicate that vulnerability-related data may be shared with specialist teams to provide appropriate support
Limit to need-to-know teams	Satisfies data minimisation. Reduces disclosure risk	Data protection policies must clearly define when/where data can be shared internally. Use tiered access.
Record lawful basis	Helps every department process consistently. Supports audits	State in policy which lawful bases used. Note any limits, e.g. 'May not be used for underwriting'
Mirror retention and erasure across systems	Prevents 'ghost copies' sitting in call recordings, case notes or Business Intelligence (BI) cubes.	Ensure data deleted/anonymised everywhere when retention timer or erasure request triggers. Document linkage in Record of Processing Activities Ideally automate processes
Keep transfer secure and traceable	Meets integrity and confidentiality obligations Supports investigations	Use role-based access in systems, not in email attachments or individual machines

9.3 Sharing across the distribution chain

Firms should share data across the distribution chain for three reasons:

- It avoids often harmful repetition of issues for the customer
- It is efficient for firms
- Consumer Duty requires outcomes to be assessed across the distribution chain, including vulnerable cohorts

To be able to share data, firms will need objective consistent data that is in a format that can be shared. This almost certainly means, it is not free-format text, not subjective and not entwined within an existing system that cannot be shared.

10 References

Chartered Insurance Institute, *Managing customer vulnerability in insurance and personal finance, a practical implementation guide* (CII, London 2025)

'Data Protection Act 2018 (c. 12)', *Legislation.gov.uk* (Crown Services, London 2018

'Data (Use and Access) Act 2025 (c. 18)', *Legislation.gov.uk* (Crown Services, London 2025

Financial Conduct Authority, *Financial Lives 2022 survey: insights on vulnerability and financial resilience relevant to the rising cost of living* (FCA, London 2022)

Financial Conduct Authority, FG21/1 *Guidance for firms on the fair treatment of vulnerable customers* (FCA, London 2021)

Financial Conduct Authority, FG22/5 *Final non-Handbook Guidance for firms on Consumer Duty* (FCA, London 2022)

Financial Conduct Authority, *Joint FCA and ICO statement on regulatory expectations regarding firms' approaches to vulnerability related data* (FCA, London 2026)

Information Commissioner's Office, 'Right to erasure', UK GDPR Guidance and Resources (ICO, London 2023)

Information Commissioner's Office, 'What are the conditions for processing?', *UK GDPR Guidance and Resources* (ICO, London 2023)

Regulation (EU) 2016/679 of the European Parliament and of the Council, Legislation.gov.uk (Crown Services, London 2016)

11 Appendix:

Appendix 1: Lawful bases for processing vulnerability data. A scenario matrix

Scenario	Description	Article 6 (personal data)	Article 9 (special category data)
Explicit consent	The customer is informed, has capacity, and freely agrees to the firm recording vulnerability data. Consent must be specific, informed, unambiguous, freely given and as easy to withdraw as it is to give.	Consent — **Art. 6(1)(a)**	Explicit consent — **Art. 9(2)(a)**
Emergency situation	Immediate risk to the customer or another person (e.g. suicidal intent disclosed on a call, active abuse, acute medical crisis) where the customer is incapable of giving consent. Narrowly scoped to the immediate protective action.	Vital interests — **Art. 6(1)(d)**	Vital interests — **Art. 9(2)(c)**
Claims, complaints and protected legal rights	Processing necessary to handle a complaint, investigate a claim, respond to a regulator or ombudsman; or establish, exercise or defend legal rights.	Legal obligation — **Art. 6(1)(c)**	Legal claims and judicial acts — **Art. 9(2)(f)**
Safeguarding of children and of individuals at risk (physical, mental or emotional well-being)	Processing necessary to protect an individual from neglect or physical, mental or emotional harm, or to protect their physical, mental or emotional well-being. The individual must be under 18, or an adult who meets the statutory definition of "at risk" (needs for care and support; experiencing or at risk of harm; unable to protect themselves as a result). Consent cannot be given, cannot reasonably be obtained, or would prejudice the protection.	Legitimate interests — **Art. 6(1)(f)**	Substantial public interest — safeguarding of children and of individuals at risk — **Art. 9(2)(g) + Sch. 1 para. 18**
Safeguarding economic well-being (adults only)	Customer meets the statutory definition of an "individual at economic risk" (an adult less able to protect their economic well-being by reason of physical or mental injury, illness or disability) and consent cannot be given, cannot reasonably be obtained, or would prejudice the protection.	Legitimate interests — **Art. 6(1)(f)**	Substantial public interest — safeguarding economic well-being of certain individuals — **Art. 9(2)(g) + Sch. 1 para. 19**
Insurance (insurance intermediaries and manufacturers only)	Processing necessary for an insurance purpose (advising on, arranging, underwriting or administering a contract; administering a claim; or exercising rights or obligations arising in connection with a contract), where the conditions in paragraph 20 are met.	Contract — Insurance — **Art. 6(1)(b)**	Substantial public interest — Insurance — **Art. 9(2)(g) + Sch. 1 para. 20**
Can't contact (only where there is a strong reason to suspect vulnerability)	Reliable indicators of vulnerability (e.g. transaction patterns, third-party disclosure) but the firm has made reasonable efforts to engage, and the customer has not responded. Recording is in the customer's interest and necessary to prevent harm and meet Consumer Duty outcomes.	Legitimate interests — **Art. 6(1)(f)**	Substantial public interest — safeguarding economic well-being — **Art. 9(2)(g) + Sch. 1 para. 19** (preferred) — or Condition 18 where the concern relates to non-economic safeguarding of an adult at risk

Note on Conditions 18 and 19: Condition 18 protects physical, mental or emotional well-being; Condition 19 protects economic well-being. Where both could apply, firms should rely on the condition that most closely matches the protective purpose. The two are not interchangeable, and each has its own statutory definition of who qualifies for protection.

12 Authors

Robert Bell

Robert Bell is founder and owner of RB Compliance Consultancy. He is an FCA and UK GDPR compliance expert and author of "A Practical Guide to the FCA's Consumer Duty". Robert has worked in compliance for many years and strives to apply a practitioner's view to all that he does.

Andrew Gething

Andrew Gething is Founder and Managing Director of MorganAsh, a leading provider of digital vulnerability management and medical underwriting services. He is a recognised expert in consumer vulnerability, driving innovation with the MorganAsh Resilience System to help firms better identify, manage and support vulnerable customers

The Chartered Insurance Institute
1st Floor, 30 Old Broad Street,
London EC2N 1HT

customer.serv@cii.co.uk
cii.co.uk

Chartered Insurance Institute

@CIIGroup

COH_J4041 (06/26)