Subject Access Request Template

Version Control

Date	Version	Change
12 March 25	1.0	Publication

Template Customisation and Usage Guide [DELETE WHEN READY]

Customising Your Policy Template

This template is a guideline and must be customised to reflect your organisation's operations, regulatory obligations, and internal controls. Replace all placeholder text with business-specific information to align with your processes, risk framework, and compliance structure.

*****This guidance and footer graphic should be removed from the final saved version*****

Using This Template

This template provides a comprehensive framework to help your organisation develop a policy that meets regulatory requirements and industry best practices. While structured to align with FCA expectations, you must review and adjust the content to reflect your organisation's compliance framework, sector-specific risks, and operational procedures.

If your organisation has policies related to this document, ensure that relevant cross-references are included. Some of the policies referenced are available separately or as part of bundled compliance toolkits.

Licence and Usage Terms

Disclaimer

This template supports regulatory compliance and governance, but does not constitute legal or professional advice. While designed for accuracy and relevance, your organisation ensures compliance with FCA regulations, industry standards, and legal requirements.

Customise this document to reflect your business model, risk exposure, and internal policies. If unsure of your regulatory or legal obligations, seek professional advice before finalising.

Use of this template assumes no liability for loss, damage, or regulatory action.

1. Introduction

Protecting personal data is not merely a legal obligation—it reflects our firm's integrity, professionalism, and commitment to treating clients fairly and with respect. As a firm authorised and regulated by the Financial Conduct Authority (FCA), we operate within a broader regulatory framework that expects high transparency, accountability, and data governance standards. This policy outlines our approach to handling Subject Access Requests (SARs) in accordance with the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and industry expectations for the financial services sector.

Subject Access Requests enable individuals to exercise their right to access personal information we hold about them. This document supplements our firm's overarching Data Protection Policy and establishes a structured procedure for managing SARs from receipt to response, ensuring that requests are dealt with lawfully, promptly, and fairly. It is intended for use by internal staff and compliance personnel responsible for processing such requests, and forms part of our broader compliance controls under the UK GDPR and FCA Principles 6 (Customers' interests), 7 (Communications with clients), and 11 (Relations with regulators).

1.1 Purpose of this Procedure

The purpose of this procedure is threefold:

1. To provide clear internal guidance on how our firm receives, validates, processes, and responds to SARs from data subjects (individuals whose personal data we hold);
2. To ensure all requests are handled in line with legal and regulatory requirements, in particular those set out under Article 15 of the UK GDPR;
3. To demonstrate, through a consistent and auditable process, that our firm is fulfilling its accountability obligations under Article 5(2) of the UK GDPR and operating with due regard for clients' rights under the FCA's Principles for Businesses and Consumer Duty expectations.

This procedure ensures we act transparently, uphold individuals' rights, and mitigate the risk of regulatory enforcement or reputational damage resulting from data mishandling.

1.2 Relationship with the Data Protection Policy

This SAR Procedure forms a standalone operational policy that complements and builds upon our core Data Protection Policy. While the Data Protection Policy outlines our approach to the lawful processing of personal data, privacy governance, and internal safeguards, this document provides the practical, procedural steps for handling individual rights requests, specifically under Article 15 of the UK GDPR (the right of access).

It should be read in conjunction with other relevant internal policies, including:

Related Policy	Purpose
Data Protection Policy	Sets out the overarching principles and responsibilities for processing personal data.
Information Security Policy	Governs controls for protecting client and staff data from unauthorised access or breach.
FCA Compliance Manual	Details how data protection obligations align with wider FCA compliance expectations, including SM&CR and conduct rules.

This relationship ensures a joined-up approach across our data governance and compliance systems, consistent with the FCA's expectations of integrated systems and controls under SYSC.

1.3 Regulatory Context – UK GDPR and the FCA Framework

The UK GDPR, enforced via the Data Protection Act 2018, provides individuals with rights over their data. Article 15 establishes the right of access, allowing individuals to obtain:

- Confirmation that their data is being processed;
- A copy of their data, and
- Supplementary information regarding the processing activities.

For firms in the financial services sector, compliance with the UK GDPR must also be viewed through the lens of the FCA's supervisory priorities. The FCA expects firms to:

- Uphold customer rights and interests under the Consumer Duty (PRIN 2A);
- Maintain robust operational resilience, including in how data is stored, accessed and recovered (SYSC 13.7);
- Ensure effective management of customer information (SYSC 9 and 4.1);
- Comply with expectations around client confidentiality, fair treatment, and data accuracy (PRIN 6 and DISP).

In practice, this means SARs must be responded to in a way that reflects not only legal requirements, but also the standards of clarity, fairness, and promptness demanded by the FCA. Our firm integrates UK GDPR and FCA expectations regimes into a harmonised compliance framework.

2. Understanding Personal Data in a Financial Services Context

In the context of a regulated financial services firm, the concept of "personal data" carries heightened importance. Not only must firms interpret personal data under the definitions set out in the UK General Data Protection Regulation (UK GDPR), but they must also factor in how this data interacts with their regulatory duties under the Financial Conduct Authority (FCA) regime, particularly with regard to conduct risk, safeguarding client assets, and treating customers fairly.

Where financial institutions collect, store, or process personal data—whether relating to individual retail clients, sole traders, partners in partnerships, staff, or directors—it is essential that the data is treated as a regulated asset. Failure to handle personal data correctly can lead to breaches of data protection law and FCA enforcement for misconduct, system and control failures, or poor treatment of vulnerable customers.

2.1 Defining Personal Data

Under Article 4(1) of the UK GDPR, personal data is defined as:

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier."

This includes (but is not limited to):

- Names, national insurance numbers, addresses, dates of birth
- Online identifiers such as IP addresses or account login details
- Identification documentation (passports, driving licences)
- Financial identifiers (bank account numbers, sort codes)
- Regulatory records (customer complaints, KYC files, call recordings)

In financial services, much of this data is collected under legal and regulatory obligations—for example, to comply with Know Your Customer (KYC) rules, Anti-Money Laundering (AML) requirements, or financial crime reporting duties under SYSC 6.1.1R.

Data becomes "personal" if it enables the identification of an individual, even when held in a broader dataset or combined with other information. This includes pseudonymised data if it could be re-attributed to an individual.

2.2 Special Category Data and Financial Sensitivity

Some categories of personal data are designated as Special Category Data under Article 9 of the UK GDPR and require heightened protections due to their sensitive nature. These include data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data

- Health information
- Sex life or sexual orientation

While financial information is not classed as special category data by default, in practice, it may be considered 'high risk' in a regulated context due to its potential for harm if breached, misused, or mishandled. The FCA treats certain types of financial data (such as income levels, debt details, or credit risk indicators) as highly sensitive, particularly when assessing firms' compliance with the Consumer Duty, vulnerability frameworks, or suitability assessments under COBS.

Furthermore, where financial data intersects with special category data—for instance, health-related expenditures disclosed in credit applications—firms may process overlapping sensitive data, triggering enhanced compliance requirements under GDPR and SYSC.

Table: Comparison of Data Sensitivity Types in FCA-Regulated Context

Type of Data	GDPR Classification	FCA Risk Consideration	Examples
Name, DOB, Address	Personal Data	Basic identifying info	Customer onboarding
Bank Details, Salary, Credit Score	Personal Data	Sensitive in financial risk and fraud terms	Creditworthiness assessments
Call Recordings, Complaint Files	Personal Data	Regulatory record – DISP implications	Quality assurance, redress analysis
Health Disclosures (e.g., in vulnerability assessments)	Special Category Data	Requires heightened protection under both GDPR and FCA Consumer Duty	Debt restructuring, affordability checks
Biometric ID (e.g., facial scan for onboarding)	Special Category Data	High data security and consent threshold	Digital onboarding platforms

2.3 Examples in FCA-Regulated Firms

To bring this into a financial services context, consider the following common examples of personal data held and processed by regulated firms:

- Insurance Firms: Customer underwriting data, medical disclosures, claims histories, and accident reports.
- Mortgage Advisors: Salary slips, tax returns, dependents, credit histories, marital status.
- Retail Investment Firms: Risk profiling data, client knowledge assessments, portfolio preferences, and financial goals.

- Consumer Credit Firms: Conducting affordability checks, reviewing income details, assessing repayment history, and identifying vulnerability indicators.
- Payment Institutions: IP addresses, device fingerprints, source of funds evidence, location data from app use.
- Discretionary Wealth Managers: KYC documentation, proof of wealth source, and ESG preferences (where processed at the individual level).

In all these instances, the data may be used to comply with the firm's regulatory obligations and tailor services, assess risk, or demonstrate fair treatment. The firm's use of this data must therefore be legally justified, purpose-limited, and proportionate to the nature of the processing activity.

3. The Right of Access under UK GDPR

The right of access, enshrined in Article 15 of the UK General Data Protection Regulation (UK GDPR), grants individuals a legal entitlement to understand how their data is used. Within FCA-regulated firms, this right sits alongside obligations under the FCA's Principles for Businesses—specifically Principle 6 (Customers' interests), Principle 7 (Clear, fair and not misleading communications), and the cross-cutting rules under the Consumer Duty. It is not simply a data protection exercise but also a matter of transparency, accountability, and treating customers fairly.

When an individual submits a Subject Access Request (SAR), the firm must confirm whether personal data is being processed and, if so, provide access to that data, as well as certain supplementary information. This right applies regardless of the firm's regulatory perimeter or the specific products or services it offers. Whether a firm is dealing with insurance clients, consumer credit customers, or retail investors, the same standard of compliance applies.

The information that must be disclosed under Article 15 is extensive. A simple data extract will rarely suffice. A firm must be ready to explain:

Requirement	Description
Whether personal data is being processed	Confirmation of processing activity, even if the data is not actively used
The purpose(s) of processing	For example, data collected for KYC, AML, marketing, or regulatory recordkeeping
Categories of personal data involved	Identification details, financial data, account activity, complaint history
Recipients or categories of recipients	Internal departments, third-party processors, regulators or auditors
Transfers to third countries	Whether data is shared outside the UK, and safeguards are in place (e.g., SCCs)
Retention periods	How long data is stored, or the criteria used to determine that period
Data source	Where the data was not obtained from the data subject directly
Existence of rights	Right to rectification, erasure, restriction, objection, and complaint
Existence of automated decision-making	Including the logic involved and implications for the individual

In firms regulated by the FCA, particular care should be taken with disclosing information involving complaint files, telephone recordings, financial assessments, and records of suitability or vulnerability. These often contain complex regulatory commentary, and it is essential that what is disclosed is intelligible and appropriate.

Where the data includes references to third parties (for example, joint account holders or staff), the firm must consider redaction or consent-based disclosure strategies to protect their privacy. Redactions must be documented and justifiable, especially if the ICO later challenges the firm.

3.1 How to Make a Subject Access Request (SAR)?

Individuals may submit an SAR by any means—written letter, email, online form, or even verbally. However, there is no formal requirement that the request reference "Article 15" or "subject access," the request must indicate that the individual seeks access to their personal information.

Firms are encouraged to provide a centralised method of contact, such as a designated SAR email address or an online portal. While verbal requests are legally valid, it is best practice to confirm such requests in writing for audit and accountability purposes.

Upon receipt, the firm must immediately record the date and trigger the internal handling process. The clock starts from the day of receipt, not from the point of internal clarification, unless further information is needed to verify identity or clarify the scope of the request. This reinforces the importance of initial intake procedures and trained staff who can recognise and escalate SARs appropriately.

3.2 What We Do When We Receive an Access Request

Once received, the firm's compliance or data protection lead must initiate the verification and fulfilment process. This is more than a clerical exercise. It requires professional judgment, internal data mapping, secure collation, and controlled disclosure.

Verification of Identity: The firm must take reasonable steps to verify the identity of the requester. In financial services, this often involves cross-checking existing KYC records or requesting certified identification. Where requests are made by third parties—such as solicitors, family members, or claims handlers—proof of authority (e.g., signed mandates or power of attorney) must be obtained and validated.

Scope Clarification: The firm may seek clarification if the request is ambiguous or overly broad. This is particularly common in large organisations with multiple systems, where narrowing the request to a specific time frame or data type (e.g., emails, call recordings, complaint files) can help avoid excessive and irrelevant disclosures.

Information Gathering and Review: The firm must conduct a coordinated search across all relevant systems—CRM tools, secure file shares, document management platforms, archived communications—and retrieve relevant data. Each item must be reviewed to determine:

- Whether it falls within the scope of “personal data”;
- Whether it contains third-party information.
- It may be exempt under legal or regulatory grounds (see Section 6).

Disclosure: The final data pack must be intelligible, structured, and provided in a secure format. For electronic disclosures, firms should use encrypted PDF files or secure portals to ensure confidentiality. Physical disclosures must be marked as confidential and sent via recorded delivery. Firms mustn't include excessive internal commentary or confidential operational notes that may breach professional secrecy or lead to reputational risk.

4. Submitting a Subject Access Request

Individuals are legally entitled to submit a Subject Access Request (SAR) to understand what personal data is held about them, how it is used, and with whom it has been shared. For firms regulated by the FCA, responding to SARs is not merely a compliance obligation under UK GDPR—it also indicates a firm's operational maturity, transparency, and commitment to fair treatment. The submission process should be clearly defined, easily accessible, and supported by internal procedures that ensure prompt and accurate responses.

Firms must accept SARs through various channels. While there is no legal requirement that the request be made in a specific format or to cite the regulation explicitly, firms are expected to recognise any expression of a desire to access personal information as a valid SAR. This includes requests submitted via customer service teams, emails to compliance departments, secure website contact forms, and even verbal requests made in branches or over the phone.

To support this, firms should maintain a single point of contact, such as a dedicated email address or a signposted web page, that allows individuals to submit their SAR in a structured manner. However, refusing or delaying the processing of a request purely because a firm's "preferred" format has not been used is not compliant with UK GDPR standards, nor acceptable under the FCA's principles of fair customer treatment.

4.1 Acceptable Formats and Contact Methods

Requests can be received in writing, electronically, or verbally. It is best practice—though not a legal necessity—for the firm to confirm verbal requests in writing to ensure clarity, reduce the risk of miscommunication, and protect both parties in the event of a dispute.

Firms should display their SAR contact details on their website and customer documentation. This includes an email address, a postal address, and an online request form where appropriate.

Method of Submission	Action by Firm
Email (general inbox or DPO contact)	Log and initiate verification immediately
Online form (dedicated SAR portal)	Automated confirmation with follow-up by the compliance team
Postal letter	Date-stamped on receipt and handed to the designated SAR handler
Verbal request (phone or in person)	Confirm details in writing and trigger the internal SAR process

Internally, staff across departments must be trained to recognise SARs and escalate them to the responsible person—usually the Data Protection Officer (DPO) or a senior compliance officer—without

delay. The statutory timeframe begins when the firm receives the request, not when it is passed to the correct person.

4.2 Verifying Identity Before Processing

Before any data is disclosed, the identity of the individual making the request must be verified. This is especially important in financial services, where personal data is sensitive and systems may include financial histories, complaint records, or KYC documentation. Verification may involve cross-referencing data held by the firm (e.g., internal client files) or requesting formal identification if there is uncertainty.

If a third party acts on behalf of the data subject, such as a solicitor, claims management firm, or relative, then authority must also be verified. This can be a signed mandate, power of attorney, or other legal instrument. Where verification is impossible or consent cannot be evidenced, the firm may lawfully decline to act until appropriate documents are provided.

The process should be documented internally. Any delays incurred due to identity verification are factored into the statutory response time only in limited cases. Firms should not use this as a justification to stall or frustrate legitimate requests.

4.3 Communicating with the Data Subject

Clear, professional communication is a cornerstone of the SAR process. Once the request has been received and identity verified, the firm should acknowledge receipt in writing. This sets the tone for the remainder of the process and demonstrates accountability.

The acknowledgement should include confirmation of:

- The expected date of response (generally within one month)
- The contact person handling the request
- Any further information needed to clarify the scope

Where clarification is required, such as narrowing the request to specific timeframes or types of interaction, the firm must approach this cooperatively and not as a mechanism to delay the response unnecessarily. Narrowing the scope will enable a more comprehensive and timely disclosure, particularly when records span multiple years or involve archived data.

5. Internal Procedure for Handling SARs

Once a subject access request has been received and verified, the firm must initiate a structured and compliant internal workflow to ensure that data is collated accurately, reviewed appropriately, and disclosed securely. For FCA-regulated firms, this process is not just a legal obligation—it also forms part of the broader governance and control framework required under SYSC and the FCA's Principles for Business. Firms must ensure that SARs are managed efficiently, with clear roles, responsibilities, and audit trails in place to evidence compliance.

The process begins with the formal logging of the SAR. Whether received by email, post, or verbally, the request must be recorded in a central SAR register maintained by the data protection lead or compliance function. This register should include the date received, the requester's name, the verification status, the response deadline, and the name of the responsible handler. This record supports internal coordination and demonstrates to the ICO and the FCA that the firm has robust controls in place for the handling of data rights.

5.1 Verification and Acknowledgement

Once the requester's identity has been verified, the firm should formally acknowledge receipt of the SAR and confirm that it is being processed. The acknowledgement should include the anticipated response deadline and a point of contact for further queries. Where identity verification is delayed, the request should not progress until satisfactory documentation has been received. Firms must be careful, however, not to impose disproportionate demands on individuals when requesting ID. what is "reasonable" will depend on the sensitivity of the data involved and the relationship between the firm and the individual.

Firms should also log whether any third party is acting on behalf of the data subject and, if so, record the authority of that party. This might include a power of attorney, a signed mandate from the individual, or a letter of instruction from a legal representative.

5.2 Data Identification and Retrieval

The central phase of the SAR process is identifying and retrieving relevant personal data. This can be complex, particularly for firms that operate across multiple systems and hold data in various formats. It is essential that all data locations—both digital and physical—are taken into consideration. These may include:

System/Source	Common Examples of Personal Data Held
Client Relationship Management (CRM)	Onboarding records, client interactions, and product applications
Secure File Storage	Scanned documents, signed agreements, and historic correspondence
Email Archives	Direct communication with clients, complaints, and advice records

Call Recording Platforms	Voice recordings from customer service, compliance, or advice calls
Case Management Tools	Complaints logs, dispute resolution files, and suitability assessments

Where applicable, archived and backup data should be searched, provided it is reasonably accessible. Firms are not expected to restore deleted data or reconstruct information that no longer exists, but they must be able to justify any gaps in the data disclosed.

The individual searching must understand the scope of "personal data" under UK GDPR and distinguish between what constitutes data relating to the individual and what is merely operational, commercial, or privileged. This distinction is crucial in complaint files, call transcripts, or advisor notes, which may contain internal commentary or references to other customers or employees.

5.3 Review and Redaction

Once the data has been collated, a second-level review must be conducted before it is disclosed. This step is crucial for ensuring legal compliance, protecting reputation, and adhering to confidentiality obligations. Where data includes references to third parties, these must either be redacted or removed unless the third party has consented or it is reasonable to disclose without their consent.

Reviewers must also ensure that no legally privileged material is disclosed inappropriately. For example, internal legal advice, MLRO case file notes, or communications relating to regulatory investigations may be exempt from disclosure. These decisions should be documented, and any redactions should be marked in the final version provided to the data subject.

Firms should take care not to withhold more information than necessary. Over-redaction can be seen as obstruction, while under-redaction can result in breaches of hird-party privacy or legal privilege Legal advice should be sought in complex or high-risk cases.

5.4 Final Disclosure and Format

The completed SAR response must be issued within one calendar month of the request. In practice, this means by the same date in the following month. If the firm cannot meet this deadline due to the complexity or volume of the request, an extension of up to two additional months may be granted, provided it is justified. The requester must be notified of this delay within the original timeframe.

Data must be provided in a structured, intelligible, and secure format. For most SARs, this will be a protected PDF file or a secure online data room. Paper disclosures are acceptable if requested. Where the SAR was submitted electronically, the response should be provided electronically unless the individual requests otherwise.

A final cover letter should accompany the disclosure pack, explaining the data provided, any redactions or exemptions applied, and the individual's rights to complain or seek correction. The DPO or compliance lead should carefully review and approve this letter.

6. Response Timelines and Fee Policy

Timeliness in responding to a subject access request is a core requirement under UK GDPR and a practical necessity under FCA expectations regarding fairness, transparency, and customer-centric service. While the law permits firms up to one calendar month to respond to an SAR, FCA-regulated entities should treat this as a maximum, not a target. A proactive compliance culture favours earlier responses wherever possible, demonstrating readiness, transparency, and strong internal control.

The countdown begins on the calendar day the firm receives the SAR, regardless of whether it was submitted to the correct individual or department. Delays caused by internal routing or slow escalation are not valid grounds for extending the timeframe. This reinforces the importance of staff training and having a clear, documented SAR escalation process.

There are circumstances where this timeframe can be legally extended, but the justification must be based on complexity or volume, not on operational capacity or staff absence.

6.1 Standard Deadlines and Extensions

The basic rule under Article 12(3) of UK GDPR is that firms must respond within one calendar month. The deadline is calculated from the day after receipt, ending on the corresponding date in the next month.

Date SAR Received	Response Deadline (One Month)
1 March	1 April
15 June	15 July
30 September	30 October

If the corresponding date does not exist in the following month (e.g. a SAR received on 31 January), the deadline is the last day of that month (e.g. 28 or 29 February).

Where the SAR is particularly complex, involving extensive records, audio files, third-party data, or multiple service lines, an extension of up to two additional months may be applied. This must be communicated to the individual within the initial month, along with an explanation of the reasons for the delay. Merely stating that “further time is needed” is insufficient.

6.2 Charging a Fee

Under UK GDPR, the default position is that information provided in response to a SAR must be free of charge. This supports the principle of fairness and accessibility and is consistent with the FCA’s expectations around open communication with clients.

However, a reasonable administrative fee may be charged:

- Where a request is unfounded or excessive, particularly if it is repetitive, or

- For additional copies of information already provided.

When considering whether a request is unfounded or excessive, the firm must take a measured and documented approach. It should not refuse a SAR or impose fees simply because the request causes inconvenience or operational burden. The threshold for “excessive” is high and may require senior-level review, particularly in regulated environments where denying access could trigger escalation to the ICO or a complaint under DISP.

6.3 Format and Method of Delivery

Unless the individual requests otherwise, the information must be provided in the same format as the request was made. If a SAR was received by email, the response should be provided electronically, usually as a secure PDF or via a secure portal. Only where paper documents are specifically requested should the firm default to printed copies.

Disclosures should be clear, well-formatted, and accompanied by a cover letter that:

Cover Letter Content	Purpose
Outline of data categories disclosed	So the recipient can understand what’s been provided
Details of any redactions or exclusions	To promote transparency
Reminder of data subject rights	Including rectification, erasure, and objection
Contact information for queries	Including an escalation route if dissatisfied

Where appropriate, the firm may offer a follow-up call or written explanation to assist the requester in understanding the data, especially if the records are complex, technical, or contain industry-specific language.

7. Additional Rights Related to Subject Access

While the right to access personal data is foundational under UK GDPR, it forms only one part of a broader suite of individual rights. These rights are not isolated; they interrelate with the firm's operational decisions, risk governance, and customer treatment standards, particularly under the FCA's Consumer Duty and SYSC obligations. It is essential that FCA-regulated firms not only recognise these rights but also build them into internal workflows and compliance frameworks.

When a data subject makes a SAR, they may also seek to exercise other rights. These must be acknowledged, assessed, and either acted upon or lawfully declined with appropriate justification. The following sections outline these rights and their application within a regulated firm.

7.1 Rectification

If individuals believe their data is inaccurate or incomplete, they can request that it be corrected or supplemented. Once such a request is received, the firm must assess whether the information held is indeed incorrect. If so, the data must be updated without delay, typically within one calendar month. The firm must also inform any third party to whom the inaccurate data was disclosed, such as credit reference agencies, insurers, or external processors, so they can also amend their records.

In cases where the firm disagrees that the data is inaccurate, it should record the individual's objection and explain the decision in writing, including the individual's right to complain to the ICO.

7.2 Erasure ("Right to be Forgotten")

The right to erasure is not absolute. It applies in specific circumstances—for example, where the data is no longer necessary for the purpose for which it was collected, where consent has been withdrawn (and no other legal basis exists), or where the data was unlawfully processed.

FCA-regulated firms often have overriding obligations to retain data under regulatory rules. These include minimum retention periods for client records, anti-money laundering documentation, complaint files, and financial transactions. In such cases, the firm may lawfully refuse the request but must provide a clear explanation of the legal or regulatory basis, which must be documented in its internal compliance records.

7.3 Restriction and Objection to Processing

Individuals may request that their data be restricted—meaning it is stored but not further processed—under certain circumstances, such as where accuracy is contested or the processing is unlawful. In practical terms, this may require the firm to flag the data internally, freeze it from automated systems, or prevent access except for strict compliance reasons.

Similarly, data subjects can object to processing based on the firm's legitimate interests or for direct marketing. While FCA-regulated firms may continue processing where there is a compelling legitimate interest, any such claim must be balanced against the individual's rights and documented with a lawful basis assessment.

7.4 Portability of Data

The right to data portability allows individuals to obtain their data in a structured, commonly used, and machine-readable format, and to transfer it to another data controller. This applies only to data provided by the individual, which is processed by automated means and based on consent or contract.

For regulated firms, this may include data, application submissions, or transaction histories. Firms must ensure they have processes in place to extract this data securely, with appropriate encryption and authentication protocols.

7.5 Rights Related to Automated Decision-Making and Profiling

If the firm makes decisions solely based on automated processing, including profiling that significantly affects the individual (such as credit approval or insurance underwriting), the individual has the right to request:

- A human review of the decision,
- An explanation of the logic involved,
- An opportunity to challenge the outcome.

Firms engaged in automated decision-making must ensure transparency about this activity in privacy notices and SAR responses. Any algorithmic logic disclosed should be described in plain language sufficient to enable meaningful understanding without revealing proprietary code.

8. Exemptions and Grounds for Refusal

While the UK GDPR provides robust rights for individuals, it also recognises that in some situations, full compliance with an SAR may not be appropriate or legally required. Exemptions exist to balance the right of access against competing obligations, such as regulatory enforcement, financial crime controls, and the rights of others.

Firms must carefully document any reliance on exemptions, with clear legal reasoning and internal review by compliance or legal personnel.

8.1 Legal and Regulatory Exemptions

Where disclosure of personal data would prejudice:

- The prevention or detection of crime,
- The apprehension or prosecution of offenders,
- the exercise of regulatory functions (such as those of the FCA),

The firm may then withhold that data. This is particularly relevant where the SAR relates to a matter under active investigation, including suspected financial crime or insider dealing.

8.2 Commercial Confidentiality and Privilege

Data may be exempt from disclosure where it includes confidential commercial information or material protected by legal professional privilege. This could include internal legal advice, minutes from the risk committee, or compliance assessments. However, firms should not use this exemption broadly to withhold embarrassing or sensitive material. Each case must be judged on legal merit, and exemptions should be proportionate.

8.3 Financial Crime Investigations and MLRO Considerations

The involvement of the Money Laundering Reporting Officer (MLRO) often introduces additional restrictions. Data related to internal SARs (suspicious activity reports), tip-off risks, or ongoing fraud reviews must be carefully ring-fenced. These records are generally exempt under the “crime and taxation” provisions of the Data Protection Act 2018 and should never be disclosed if doing so would prejudice an investigation.

8.4 Notification and Explanation Obligations

Where the firm relies on any exemption or refuses to comply with a SAR in whole or in part, it must still provide the individual with:

Notification Requirement	Purpose
Confirmation of non-disclosure	So the individual understands that their request has been limited

Reason for refusal or exemption	Including legal reference and, where applicable, an explanation of prejudice
Right to complain to the ICO	Ensures due process and transparency

This information must be delivered within the standard response timeframe and in a clear and intelligible format.

9. Complaints, Appeals and Regulatory Contact

Effective complaint handling reinforces a firm's accountability under UK GDPR and aligns with FCA expectations for transparent client communication. Where a data subject is dissatisfied with the outcome of their SAR or how it was handled, they must have a clear route to raise a formal concern internally and escalate it externally if necessary.

9.1 Internal Complaint Escalation

Individuals who wish to raise concerns about handling their SAR should be encouraged to contact the firm's Data Protection Officer or Compliance Lead in the first instance. The complaint should be acknowledged within five working days and investigated promptly, with a written outcome provided within 28 days wherever possible.

Internal complaints must be logged and reviewed periodically to identify procedural gaps, training needs, or systemic failings.

9.2 Contacting the Information Commissioner's Office (ICO)

Where an individual remains dissatisfied, they have the right to complain to the ICO. Firms should provide the ICO's full contact details and any refusal notices in the SAR response letter. Firms should also co-operate with the ICO in any investigation and use findings as opportunities for improvement.

ICO Contact Details	
Address	Wycliffe House, Water Lane, Wilmslow, SK9 5AF
Telephone	0303 123 1113 or 01625 545 745
Email	enquiries@ico.org.uk
Website	www.ico.org.uk

9.3 Contact Details for the Company

All SARs and related correspondence should be directed to:

Data Protection Contact	[Insert Name]
Company Name	[Insert Name]
Address	[Insert Address]
Email	[Insert Email]
Telephone	[Insert Phone]

These details should be outlined in the firm's privacy notice, SAR form, and on the website.

9.4 EU Representative (if applicable)

Where the firm offers services to individuals in the EU and is not established in the EU, it must appoint a representative in accordance with Article 27 of the UK GDPR. The representative's contact details should be disclosed in the privacy policy and SAR correspondence to allow EU-based individuals to exercise their rights effectively.

10. Record-Keeping, Monitoring and Review

The UK GDPR's accountability principle requires firms to comply with rights-based obligations and demonstrate how they maintain that compliance. FCA-regulated firms are also expected to maintain clear governance structures and conduct regular monitoring to uphold data rights consistently.

10.1 Record of Requests

Each SAR received must be logged in a centralised register. This should include:

- Date received
- Requester's identity
- Response due date
- Final response date
- Outcome (full disclosure, partial, or refusal)
- Any exemptions applied

This record should be reviewed periodically to assess its timeliness, consistency, and overall effectiveness in control.

10.2 MI and Reporting to Governance Forums

Management Information (MI) on SAR volumes, types, and outcomes should be included in compliance reporting to governance bodies. Repeated requests or patterns (e.g. high volumes from a specific client group) can indicate underlying dissatisfaction or possible risks that warrant further review.

10.3 Annual Review and FCA Alignment

This procedure should be reviewed at least annually, following any material regulatory or legal change. Firms must ensure that their SAR processes align with current UK GDPR obligations and FCA expectations, including those under the Consumer Duty and SYSC.

10.4 Training and Awareness

Staff who handle SARs—especially front-line staff and those in compliance or data protection roles—must receive appropriate training. This includes:

Audience	Training Focus
Front-line staff	Recognising SARs and routing correctly
Compliance/DPOs	Applying exemptions, redactions, and disclosure controls
Senior management	Oversight, governance, and risk mitigation

Training should be refreshed annually and documented as part of the firm's broader SM&CR and data protection training framework.

11. Appendices

Appendix A – Subject Access Request (SAR) Template

You have the right under the UK General Data Protection Regulation (UK GDPR) to request a copy of the personal data that [Insert Firm Name] holds about you, as well as supplementary information about how your data is used. This form is designed to help you exercise that right.

Please complete all relevant sections to help us process your request efficiently. If you require assistance completing this form, contact our Data Protection Officer at [insert email address].

Section 1 – Your Details

Please provide your full name and current contact details. We will use this information to verify your identity and respond to your request.

Field	Your Response
Full Name	
Any Previous Name(s) Used	
Date of Birth (DD/MM/YYYY)	
Address	
Postcode	
Email Address	
Contact Number	

Section 2 – Verification of Identity

We are required to verify your identity before releasing any personal data. Please provide a scanned or photocopied copy of two forms of identification. One must provide a photographic ID (e.g., passport or driving licence), and you must confirm your address (e.g., utility bill or bank statement dated within the last three months).

Accepted ID Types	Examples
Photographic ID	Passport, Driving Licence
Proof of Address	Utility Bill, Bank Statement

We will destroy copies of identification securely once the request has been fulfilled.

Section 3 – Details of Your Request

To help us locate your data efficiently, please describe the information you wish to access. Include relevant dates, account numbers, or interaction types (e.g., phone calls, complaints, emails).

Question	Your Response
Please describe the data you are requesting	
Period covered by the request	
Relevant account or customer reference numbers	
Specific departments or teams involved	
Preferred format for receiving the data	☐ Email ☐ Post

If you do not specify a time range, we will provide all data held that falls within the scope of UK GDPR.

Section 4 – Third Party Requests

Complete this section only if you are acting on behalf of someone else (e.g. solicitor, relative, claims manager).

Acting on behalf of: [Full name of data subject]

Relationship to the individual

Authority to act (enclose one): ☐ Signed Mandate ☐ Power of Attorney ☐ Letter of Instruction

We may contact the individual directly to confirm your authority before releasing any information.

Section 5 – Declaration

By signing below, you confirm that the information provided in this form is accurate and that you are entitled to request access to the personal data specified above.

Signature	
Name (Print)	
Date	

If submitting electronically, please type your name above to indicate your consent.

Submission Details

Please return this form and identification documents to:

Data Protection Officer

[Insert Company Name]

[Insert Address Line 1]

[Insert Address Line 2]

[Insert Town/City, Postcode]

Email: [Insert email address]

Phone: [Insert phone number]

We will respond to your request within one calendar month of receipt, subject to identity verification and any clarifications required. If your request is complex or involves a high volume of data, we may extend the deadline by up to two months. You will be notified in writing if this applies.

Data Protection Statement

This form and the information submitted with it will be used solely to process your request and fulfil our obligations under the UK GDPR. It will be securely stored and deleted in accordance with our retention policy.

Appendix B – Identity Verification Checklist

Purpose

This checklist must be completed and retained for every Subject Access Request (SAR) received by the firm. Its purpose is to ensure that personal data is not disclosed to unauthorised individuals and to evidence compliance with the firm's obligations under the UK GDPR (Articles 12 and 15), as well as FCA Principle 6 (Customers' Interests) and Principle 10 (Clients' Assets and Information).

SAR Reference Number:

[Insert internal reference or case ID]

Date SAR Received: [DD/MM/YYYY]

Handler Name: [Insert name of reviewer]

Verification Completed On: [DD/MM/YYYY]

1. Identity of Data Subject

Verification Item	Acceptable Evidence	Verified? (Y/N)	Notes
Full legal name matches request	Photographic ID (passport, driving licence)		
Current address matches firm records	Utility bill or bank statement (last 3 months)		
Date of birth confirmed	ID document or firm's KYC data		
Email address or phone number verified	Matches the firm's client file		

If identification does not match internal records, do not proceed with the SAR. Escalate to the DPO or compliance officer.

2. Identity of Third Party Representative

(if applicable)

Verification Item	Acceptable Evidence	Verified? (Y/N)	Notes
The full name of the third party matches the request	Photo ID and contact details		

Evidence of authority to act	Signed mandate, letter of authority, power of attorney		
Confirmation from the data subject (if required)	Separate written confirmation from the subject		

Note: A legal mandate is required unless the third party is a parent of a minor, legal guardian, or attorney under a registered power of attorney. Where authority is unclear, pause, request and seek clarification in writing.

3. Internal Validation Checks

Internal Check	**Outcome**
Identity documents reviewed and authenticated	☐ Yes ☐ No
All documents are stored securely	☐ Yes ☐ No
Identity verified to a reasonable standard	☐ Yes ☐ No (Escalate to DPO)

4. Authorisation to Proceed

Final Authorisation	
Identity verification complete	☐ Yes – proceed with data retrieval
Handler Signature	
Date	
Reviewed by (Compliance/DPO)	
Date	

This completed checklist should be stored with the SAR case file and retained in accordance with the firm's Data Protection Policy and internal SAR register procedures. Documents provided for identity purposes must not be retained longer than necessary and should be securely destroyed once verification is complete and the SAR has been fulfilled.

Appendix C – Redaction Guidelines

Purpose

Redaction is the process of obscuring or removing specific information from documents before they are disclosed, in order to protect the privacy of third parties, maintain confidentiality, or comply with legal restrictions. Within FCA-regulated firms, redaction must be undertaken carefully and justifiably, mainly where internal records include discussions of suitability, complaint assessments, or internal risk reviews.

When to Apply Redaction

Redactions must be applied when:

- Personal data of individuals other than the requester is not disclosed and cannot be lawfully disclosed.
- Information is protected by legal privilege (e.g. legal advice or regulatory communications).
- Disclosure would prejudice criminal investigations, anti-money laundering reviews, or internal investigations into misconduct.
- Data is commercially sensitive or reveals firm methodologies, financial models, or pricing strategies that are inappropriately disclosed.

Redaction must never be used to conceal poor practice, adverse findings, or to frustrate transparency unless one of the above exemptions applies.

Redaction Procedure

All redactions must be reviewed and signed off by a second compliance team member or the DPO. The redaction process must follow these steps:

1. Identify personal data belonging to third parties.
2. Consider whether consent has been obtained or whether disclosure is necessary and lawful.
3. Remove or redact non-disclosable content using secure software.
4. Insert a clear marker (e.g. “[REDACTED – Third Party Data]”) indicating redaction.
5. Maintain an internal log of redactions applied, including the justification for each.

Examples of Common Redaction Scenarios

Type of Information	Redact?	Justification
Another customer’s name is in the complaint file	Yes	Third-party data – cannot disclose without consent
Advisor’s internal notes or speculation	Case-by-case	If data relates to a client, retain; if operational or defamatory, redact

Internal email chains	Case-by-case	Redact the names of staff if not relevant to the data subject
FCA communications or legal advice	Yes	Protected by privilege or regulatory function

All redacted documents must be retained in both their redacted and original forms for audit and evidentiary purposes.

Appendix D – Internal Workflow Map for SAR Processing

This map outlines the operational steps a firm should follow when receiving and responding to a SAR, ensuring regulatory compliance, operational clarity, and internal accountability.

Step	Action	Responsible Function	Timeframe
1	SAR received via email, portal, post, or in person	Front-line / Support / DPO	Day 0
2	Record SAR in the central register	Compliance / DPO	Within 24 hours
3	Acknowledge the request in writing	Compliance / DPO	Within three working days
4	Verify the identity of the requester and any third-party representative	Compliance / Legal	Before progressing
5	Clarify the scope with the requester if required	Compliance / Operations	Within five working days
6	Retrieve data across all relevant systems	IT / Operations / Data Owners	Within 10–15 working days
7	Review data, redact where appropriate, apply exemptions	Compliance / DPO	Within 5–10 working days
8	Prepare final pack, write cover letter	Compliance / DPO	Day 25–28
9	Issue a SAR response securely to the requester	Compliance	Within one calendar month
10	Update the SAR register, destroy ID documents securely	Compliance / DPO	Post-response (retain core log)

All staff involved must maintain a clear audit trail throughout the process. Internal deadlines must be tracked in MI reports and shared with governance forums.

Appendix E – Key Definitions and Legal References

This section provides standard definitions and core legal references to support consistent understanding across all SAR handlers and internal reviewers.

Key Definitions

Term	Definition
SAR (Subject Access Request)	A request from an individual to access their data under UK GDPR Article 15.
Personal Data	Any information relating to an identified or identifiable natural person.
Data Subject	The individual to whom the personal data relates.
Processing	Any operation performed on personal data, including storage, retrieval, or disclosure.
Controller	The organisation that determines the purpose and means of processing personal data.
Redaction	The act of obscuring or removing data from documents before disclosure.
Third Party	Any individual or organisation other than the data subject and the controller.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, health, and other similar information.
ICO	The Information Commissioner's Office – the UK's independent data protection authority.

Legal and Regulatory References

Document	Relevance
UK GDPR (Regulation (EU) 2016/679 as retained in UK law)	Sets out rights of access, controller obligations, and processing standards.
Data Protection Act 2018	Supplements UK GDPR with national provisions and lawful bases.
FCA Handbook (especially PRIN, SYSC, DISP)	Outlines expectations for regulated firms regarding client treatment, systems, and controls.
ICO SAR Guidance	Provides a practical interpretation of SAR handling under UK GDPR.

Article 15 of UK GDPR	Core legal basis for SARs and associated obligations for controllers.

End.