fair4all finance

Good Practice Lending Guide

RM12 Data Maintenance and Retention

May 2024

Disclaimer

This Guide is provided purely for informational purposes, has been prepared for general use only, and does not constitute legal, financial or other professional advice.

All information contained in this Guide is based on the laws and regulations applicable to England and Wales and which are current as of the date of publication. This guide is not maintained regularly, but we will endeavour to update it when relevant laws or regulations are amended, varied, or supplemented. At a minimum, the Guide will be reviewed annually to ensure compliance with any legal or regulatory changes.

Fair4All Finance Limited make no representations or warranties of any kind, express or implied, about the accuracy, completeness, suitability, or reliability of the information contained herein. Fair4All Finance Limited shall not be liable for any loss or damage arising from the use of, or reliance on, this Guide. This Guide does not create an advisor-client relationship between you and Fair4All Finance Limited.

You are advised to consult with suitably qualified legal, financial or professional advisors to obtain advice tailored to your specific circumstances. You should not rely on the content of this Guide and any reliance on any information provided in this Guide is done at your own risk.

By accessing and using this Guide, you acknowledge and agree to the terms of this disclaimer.

This Guide must not be amended, copied, reproduced, distributed or passed on at any time without the prior written consent of Fair4All Finance Limited.

Contents

1 Introduction

1.1 What are data maintenance and retention, and why are they important?

Without good quality data about its customers a lender is operating in the dark. Operationally, data is essential for managing customers' accounts and interacting with them. This is to ensure that both parties are meeting the terms of their credit agreements and to ensure good outcomes for customers in line with the FCA's Consumer Duty principle. Accurate and detailed customer records also provide an audit trail of the interactions lenders have with their customers. This is needed if customers have queries or complaints about their accounts, and for evidencing good business practice to auditors and regulators.

From a management perspective, customer data is a key ingredient for management reporting that informs the business about how it is performing. Similar data is also needed for regulatory reporting to the PRA/FCA. Consequently, maintaining extensive and detailed customer records, about how they behave and their interactions with the business, are vital to enable good, data driven, business decisions to be made.

Maintaining comprehensive customer information is vital for managing a lending business effectively. However, lenders must also ensure that they respect and manage their customers' personal data in line with data protection law.

In the UK, any organisation that deals with personal data must be registered with the Information Commissioner's Office (ICO) and ensures it complies with the Data Protection Act 2018. The bulk of the personal data held by a credit union or other lender will be customer data, and customer data is the primary focus of this document. However, lenders should be aware that the Data Protection Act applies equally to any other personal data that lenders hold such as employee records, contact lists used for marketing and details of supplier contacts.

The Data Protection Act 2018 is the UK's implementation of the EU's General Data Protection Regulation (GDPR) which the UK was required to implement when it was member of the EU and has subsequently been retained following Brexit[1]. Most people refer to "GDPR" rather than "the Data Protection Act", and this convention is adopted throughout the rest of this document.

The ICO has the power to fine companies up to £17.5m or 4% of global turnover (whichever is higher) if

[1] The ICO often refer to "UK GDPR" to reflect the fact that the UK's data protection laws could diverge from those of the EU in future.

found in breach of GDPR. The ICO can also issue enforcement notices to make organisations comply with GDPR or to stop processing customer data altogether.

Given the nature of the products and services they provide, any lender providing consumer credit, including loans, credit cards and mortgages will be dealing with considerable volumes of personal data daily. For many customers, this will include special category[2] data about their health or other vulnerabilities. Consequently, data protection compliance should always be a high priority and every lender should have a designated Data Protection Officer (DPO) responsible for ensuring the organisation's compliance with GDPR.

Poor data management can also contribute to action and fines by the Financial Conduct Authority (FCA), the Prudential Regulatory Authority (PRA) or the Financial Services Ombudsman (FOS), if a company can't evidence what it has done or provide accurate regulatory reporting. For example, Goldman Sachs were fined more than £30m in 2019 by the FCA, and Metro Bank more than £50m in 2021, for failures in their regulatory reporting.

1.2 Why has Fair4All Finance commissioned this guide?

In our work with community finance lenders, those we have made significant investments into, and those we have funded through grants and capability support, we have come across a range of approaches to data maintenance and retention.

This guide reflects our intention to document what good practice looks like for data maintenance and retention to share the insight that has been developed for specific lenders more broadly.

1.3 Purpose and scope of this document

GDPR covers all aspects of personal data, how its gathered, held and used. This element of the Guide describes good practice when it comes to data maintenance and retention. This covers how personal data should be managed by lenders and how long that data should be held to enable them to undertake the activities required to run their business effectively, while also complying with GDPR and other regulation. Details about how personal data should be treated as part of the application process is described in the Application Process (RM03) component of the Guide.

Every lender has their own data requirements for running their business. However, it is important that lenders clearly define and comprehensively document their requirements for personal data in terms of what data they hold, how they maintain the accuracy of that data and how they ensure they only retain data for as long as they need it.

[2] Data that is deemed under GDPR to require extra care when processing to avoid causing customer harm.

The approaches to data maintenance and retention described here are generally applicable to all UK lenders, but it is primarily intended for small to medium sized organisations who are working to provide fair and affordable credit to sectors of the community who may otherwise struggle to obtain it. For example, not-for-profit community lenders and credit unions. Therefore, it adopts a proportionate approach suitable for these types of organisations.

The focus of this document is customer data, but the same principles apply to any other personal data an organisation holds. For example, staff records, payroll information and supplier documentation (eg contact details).

Organisations can use the Guide in one of two ways:

1. As a reference manual, to help them enhance their own policies and processes to provide assurance that there are no gaps or shortcoming
2. To support new organisations in setting up appropriate data maintenance and retention processes

The focus of this document is data maintenance and retention in line with the requirements of GDPR. However, there are clear overlaps with other areas of lending, such as assessing new loan applications, arrears processing, credit reference agencies etc. These are signposted within the relevant sections throughout this guide.

2 Data protection principles

In this section the areas of GDPR that are relevant to data maintenance and retention are discussed.

2.1 Permissions (consent)

To hold or process[3] an individual's personal data, an individual must have given their consent[4]. Therefore, a lender will provide a clearly worded privacy notice to the customer at the start of the loan application process, detailing how their data will be used[5]. The customer must agree (give consent) to the use of their data for the purposes stated in the privacy notice before the loan application can proceed further. Consent for each purpose that their data will be used for must be explicitly provided by the customer. Consent cannot be assumed or hidden away in the small print of a contract or terms of business.

This means that additional consent may need to be sought from customers whenever:

1. An organisation decides it wants to do something new with the customers data that the customer has not previously provided consent for
2. An organisation wants to obtain new data to use in an existing process, and it has not previously informed the customer about this

An example of the first point is a lender who has entered into an agreement with a second lender to pass on details of loans applications that were marginally declined. The second lender could potentially lend to these cases because they have a greater risk appetite and provide products that are more suitable for these customers. However, this agreement can only be enacted if the customer has consented to their details being passed to the second lender. This consent is not currently provided. Therefore, the lender decides to redesign its application process to seek consent from declined customers to allow them to do this[6].

An example of the second point is a lender who decides they want to seek a refreshed credit report each

[3] Under GDPR "storing" or "holding" data is also classified as processing.
[4] GDPR Article 4(11).
[5] For credit unions, the consent required for the managing of loans may have been contained in the original membership application.
[6] The lender decides to only ask for the customers consent at the decline stage to "unbundle" the request from the main loan application. See GDPR Recital 43.

month for all loan customers to support their customer management process. They want to use the credit report to identify customers who may be struggling with other debt commitments so that they can include this information in their pre-delinquency strategy[7]. Consequently, the lender adds an appropriate statement to the privacy notice that is presented during the application process, to state that the credit report may be refreshed at regular intervals.

Further information about privacy notices is provided in the Proposition Design module of the Guide.

Good practice is for lenders to maintain a record (an inventory) of the personal data they hold, the source of that data and what permissions have been given around the use of that data. This can then be referenced whenever an organisation changes how it processes data or wants to use that data for a new purpose. Data inventories are discussed in more detail in Section 3.

2.2 Data accuracy

Firms must ensure that the data they hold about individuals is accurate[8]. The GDPR does not define "accuracy." but as the ICO comments, it should be obvious in most cases if data is accurate or not[9].

In practice, the ICO does not expect all data to be accurate all the time, only that:

- Robust processes exist to check and validate personal data when it is first collected
- There is a process to correct data errors promptly when they are found
- There are ongoing audit/validation processes in place to monitor the accuracy of data, with action undertaken if any problems are found

For example, when someone provides their date of birth as part of a credit application, the application processing system should automatically validate that the date is a real date. Also, that it's not today's date or a date in the future. The system also produces warnings if the date of birth is very recent or very old, implying someone is aged say, <16 years or >100 years old[10]. After a loan is granted, if a customer reports that their date of birth is incorrect, then it is corrected promptly (and ideally immediately). The company also performs annual audit checks on the quality on the date of birth field to ensure that it is fully populated with valid dates.

[7] See the Arrears and Collections Component of the Guide for more information about pre-delinquency and how to deal with it. Note also that this would be a "soft search" that would not impact the customers credit report.

[8] GDPR Article 5(1)(d)

[9] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/#accuracy_principle

[10] These are somewhat arbitrary but represent the maximum and minimum that could reasonably be expected. "Correct" applications from young adults say, 16 or 17 years old, may be received. These are valid cases from a data perspective but are declined later down the line due to lending policy (Decline all applications from <18s).

2.3 Requests for data

2.3.1 Subject Access Request (SAR)

Under GDPR, an individual has a right to Subject Access. This means they can demand a copy of any or all the data that an organisation holds about them.

The information must be supplied in a format that is understandable by a layperson with supporting notes if required. For example, if someone's employment status is recorded as 1,2,3,4,5 then the meanings of these codes must be supplied (1=employed, 2=part-time, 3=retired and so on).

This means that an organisation needs to:

- Maintain a record of what data they hold and what the data means
- Have a process of securely collating the data they hold into a format that can be delivered to the individual making the request

Subject access requests include any inferred or derived data that an organisation maintains. For example, if a lender calculates certain scores or metrics about its customers, these also need to be provided and explained. Some examples of these include credit scores calculated by the firm, debt to income ratios, and age (derived from date of birth – so technically both age and date of birth would need to be provided if it was within the scope of the subject access request).

When making a subject access request, an individual is legally entitled to a copy of every piece of data that an organisation holds about them. This includes "non-standard" data such as security footage and voice recordings. Gathering all this data can be a costly and time-consuming task, particularly for smaller organisations for whom such requests might be a highly manual process. However, in most cases, the individual is seeking answers to a specific issue or concern that they have. If the lender can establish precisely what information they are looking for and why, then they can save considerable time by agreeing this with the customer.

For example, if the issue is with a recently declined loan application, the customer may not need or want information about all the other loans they had in the past – just the reasoning around the decline decision for this loan. Consequently, a well-designed subject access process which includes a questionnaire or checklist to identify the information required can reduce the cost of subject access requests considerably.

Firms must respond to a subject access request within 1 calendar month[11] from receipt of the request[12].

2.3.2 Right to data portability

The right to data portability is somewhat like a subject access request but covers only personal data provided by the individual themselves. Data that has been obtained from other sources and derived data are not covered.

A key difference is that the right to portability gives individuals the right to receive personal data they have provided to you in a structured, commonly used, and machine-readable format. Examples of machine readable format include CSV files and XTML. This contrasts with a subject access request where the data could be provided in a paper format or as a document that is not "machine readable."

The right to portability also provides individuals with the right to request that a lender transfers their data directly to another organisation.

2.4 Right to be forgotten (erasure)

Individuals have the right to have their data erased[13]. This is commonly known as the "Right to be forgotten." This includes data held on backup systems as well as the current live systems.

This right is not universal and does not apply if the data has been obtained lawfully and is necessary for the purposes of dealing with the customer. For a loan provider, this means that the customer would not be able to exercise the right to delete their customer records if they are required to manage the running of their account, or information about old, closed accounts if they need to be retained to meet legal or regulatory requirements.

For example, customers are allowed to raise complaints with lenders up to 6 years after a problem occurs with their account[14]. It can then take up to 8 months for the customer to dispute the lender's findings and escalate the complaint with the Financial Services Ombudsman (FOS)[15]. It will then take the FOS some time to investigate. Therefore, it is not unreasonable for lenders to have a policy of maintaining customer records for *at least* 7 years after account closure.

An example where the right to be forgotten could be enacted would be if a customer wasn't a credit union member but was on a mailing list used by the credit union to contact people who might be interested in joining.

[11] If the SAR is complex, or an individual makes multiple SARs in a short period of time, then the response period can be extended to 3 months, but the individual must be notified about the extension within 1 month of their initial request.
[12] A SAR request can be made verbally or in writing.
[13] GDPR Article 17.
14 https://www.financial-ombudsman.org.uk/consumers/expect/time-limits
[15] Lenders must provide a final response to a complaint within 8 weeks. The customer then has 6 months to raise a FOS case.

2.5 Security

GDPR requires personal data to be:

> Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures[16]

It is up to each organisation to determine how best to comply with the security requirements of GDPR but the general principles that all organisations should adhere to are:

- **Restricted access**. People only have access to the types of personal data that they need to do their job. This is not an issue of seniority but job role. Just because a member of staff is more senior does not mean they have greater access. A junior call centre operator may need greater access to individuals' data than the CEO
- **Data encryption.** All personal data is encrypted as standard
- **Secure data transfer**. Personal data is not sent by ordinary e-mail/text, even within the company. Where data transfers are required, these are undertaken via controlled and secure means. For example, dedicated SharePoint sites or Secure File Transfer Protocols (SFTP). For the best security, files (such as an Excel file containing a list of customers in arrears) are also encrypted and password protected even when a secure data transfer route exists
- **Backups**. These are required to protect against accidental loss or deletion of data
- **Physical security.** Most data these days is electronic, but one route for data to be compromised is via access to physical assets (buildings and IT equipment) that allows data to be accessed. Therefore, appropriate controls over who can enter an organisation's sites and has access to laptops and other equipment needs to be controlled so that only permitted staff, who need access to undertake their roles, have access. Mobile devices such as laptops and phones should also have suitable access controls, such as passwords or fingerprint scanners. Likewise, any paper documentation should be held in a lockable storage medium (eg filing cabinet)
- **Data disposal.** All media, be it paper or electronic, is disposed of in a suitable manner. This means that the data is destroyed beyond any means of recovery. Where IT hardware is involved, this may mean destroying hard drives before the equipment is sold or recycled
- **Regular review.** Security procedures are regularly reviewed

Further details of the ICOs expectations regarding data security are provided on the ICO website:

[16] GDPR Article 5(1)f

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/#6

3 Data inventory

To comply with Article 30 of the GDPR, lenders need to maintain a record of processing activities, that is, an inventory of the personal data they hold and how it is used (processed).

As a minimum, to comply with Article 30, the inventory should include the items in Table 1, for each type of personal data:

Table 1. Data Inventory Requirements (GDPR Article 30)

Inventory Item	Description
Business function	The area of the business that uses the data. For example, underwriting, HR, customer management, fraud department, procurement and so on
Reason for processing	This describes what the business function will do with the data eg loan underwriting, arrears management, cross-selling other products, and services
Category of individual	For example, existing customers, declined applicants, former customers, staff, suppliers etc.
Category of data	This describes the types of data used for processing. For example, contact details, credit report, bank details and so on.
Data source	Where the data originated from. For example, the customer directly, a government service (such sanctions and PEP lists) or a credit reference agency
Third party access	This details any external organisation who may have access to the data. For example, credit reference agencies need to be given peoples' name, address, and date of birth to be able to perform a credit search and provide a credit report.
International transfers	This identifies where the data will be transferred outside of the UK/EU. For example, to a supplier that processes data in the US
Retention period	Details of how long data should be held for before it is deleted (or anonymised). This should align with the information detailed in the firm's retention policy (See section 5)
Security measures applied	How the data is stored to ensure that the data is secure. For example, that the data is encrypted, stored in secured cabinets, access controls exist and so on

Note that an organisation may also wish to include other GDPR relevant information in the inventory, such as the source of legal basis to process data (such as via a contract, customer consent, or legitimate interest[17]), if the data is classified as a special category and so on.

Maintaining an up to date inventory is important because it supports many other activities required for GDPR compliance. If we think back to the areas covered the previous section, all of these are facilitated by having a good quality and up to date data inventory.

A partial (fictional) example of a data inventory is shown in Table 2.

[17] Legitimate interest is one of the six lawful bases for processing personal data. Legitimate interests is more flexible than the other principles and can in principle apply to any type of processing for any reasonable purpose. For further information see the ICO website. What is the 'legitimate interests' basis? | ICO

Table 2. Data Inventory Example (Extract not full example)

Business function	Purpose for processing	Category of individual	Category of data	Data Source	Third party access	International transfers	Retention period	Security measures
Membership	Membership management	Member	Membership details	Customer	CRA / Open banking	N/A	7 years after membership ends	Encrypted, Access Controls, Secure Transfer (SFTP)
Underwriting	Verification and affordability	Member	Bank statements (Open banking data)	Customer's bank	N/A	N/A	7 years after loan completion.	Encrypted, Access Controls
Underwriting	Credit risk assessment	Member	Credit report	The XYZ credit reference agency	CRA	N/A	7 years after loan completion.	Encrypted, Access Controls, Secure Transfer (SFTP)
Underwriting	Credit risk assessment	Member	Application credit score	Derived (from App. and CRA data)	N/A	N/A	7 years after loan completion.	Encrypted, Access Controls
Customer management	Account management	Member	Membership details	Customer	Debt collection agencies	N/A	7 years after loan completion.	Encrypted, Access Controls, Secure Transfer (SFTP)
Customer management	Account management	Member	Account records	Internally generated	Debt collection agencies	N/A	7 years after loan completion.	Encrypted, Access Controls, Secure Transfer (SFTP)
…	…	…	…	…	…	…		
Finance	Payroll	Staff	Contact details	Employee	HMRC, Pension provider	N/A	6 years	Encrypted, Access Controls
Finance	Payroll	Staff	Bank details	Employee	HMRC, Pension provider	N/A	6 years	Encrypted, Access Controls
Finance	Payroll	Staff	Pension details	Pension provider	HMRC, Pension provider	N/A	6 years	Encrypted, Access Controls
…	…	…	…	…	…	…	…	…
HR	Recruitment	Job applicants	Contact details	Job applicant	Disclosure and Barring service (DBS)	N/A	3 years	Encrypted, Access Controls
HR	Recruitment	Job applicants	Employment history	Job applicant	N/A	N/A	3 years	Encrypted, Access Controls
HR	Recruitment	Job applicants	Criminal record check (CRC)	DBS	N/A	N/A	3 years	Encrypted, Access Controls
…	…	…	…	…	…	…	…	…

Note that:

- In Table 2, related items are grouped together by category. In theory, a lender could have separate entries for membership number, name, address, phone number and e-mail. However, it is fine to group these as "membership details". This is because these items are all used for the same types of purpose
- Where a category of data is used for more than one purpose, that data is recorded against each purpose. In the above example membership details are repeated several times
- The data inventory should include derived information. If a lender creates flags or indicators to represent certain customer conditions or scores, these should be covered
- Some columns are not relevant for this organisation but are included for completeness. For example, the international transfers column is included, even though there are no data transfers performed by the firm

It is up to each organisation to define their own data inventory, but the ICO also provide a template for organisation to use and an example of a populated template on their website[18].

3.1 Meta data

Meta data can be defined simply as "data about data." Anything that tells you something about a piece of data, what it means, how it's stored or used can be described as meta data. The information contained in a firm's data Inventory is one form of meta data that provides information about the source and uses of each category of data.

To further support GDPR, lenders should also have additional meta data defined in a data dictionary. A data dictionary details the source, format and meaning of each individual item of personal data (and other data[19]) that they hold. This type of meta data is particularly useful for explaining the data an organisation holds when a subject access request is received.

Where data is stored as codes, flags, or indicators then the meaning of each value needs to be stated in common language in the data dictionary. For example, if there is an indicator called "Suspected fraud" that can take values of A, B or C, then the document should state that A means "Proven Fraud", B means "Suspected Fraud", and C means "Not Fraudulent".

Even where the contents of the fields seem obvious such as a numeric data item called "Age of Customer"

[18] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/documentation/how-do-we-document-our-processing-activities/

[19] To support good running of the organisation all data should have meta data contained in the data dictionary, not just personal data.

some level of metadata will be required. Some organisations hold age in years, some in months and some as years and months. The meta data should state which convention is applied. Similarly, some organisations use default values if the age is unknown or missing, such as -1 or 999. The meaning of these default value should also be explained in the data dictionary.

There is no specific format that a data dictionary should have, but good practice is that it should provide a complete description of each data item, its source, format, and range of values it can take. A (fictional) example of part of a data dictionary is provided in Table 3.

Table 3 Example of a Data Dictionary

Database / Table	Field name	Description	Format	Values	Source	Notes
Applications	D_O_B	The applicant's date of birth	Character length 8 in DDMMYYYY format.	01010001 - 31129999	Application form	Checks occur during data entry to prevent illegal dates or characters being entered
Applications	Res_Status	The applicant's residential status	Integer length 2.	0 = unknown / other 1=Homeowner 2=Renting 3- Living with parents 4=Institution	Application form	Note that the field format was changed in October 202x from character to integer
Applications	Income	The applicant's gross monthly income as declared on their application form in £	Integer (no decimal places) length 8.	0 - 99999999	Application form	0 is valid 99999999 = unknown
Applications	CScore	The XXX credit score provided by YYY CRA	Integer length 4.	-1 = no trace. 0 - 999	Credit reference agency	The CRA implemented a new score in March 202x. The old score used -99 to represent no trace
Applications	Sanctions	A flag to indicate if the customer matches to the Sanctions list	Character length 1	Y = sanctions match N= Not sanctions match	UK Gov sanctions list	This flag indicates that further checks should be made, not that the person is confirmed as sanctioned
....	....	....	....	....	....	....
Customer management	D_Date	The payment due date as per the loan agreement.	Integer length 2.	1 - 28	Internal	Only days that appear in all months permitted
Customer management	Balance_1	The customer's original loan advance + fees	Real number (two decimal places) length 8.	-99999.99 = Account closed fully paid.	Internal	
Customer management	Balance_2	The customer's outstanding loan balance as at last month end	Real number (two decimal places) length 8.	-99999.99 = Account closed fully paid.	Internal	
Customer management	Balance_3	The customer's current (live) outstanding loan balance	Real number (two decimal places) length 8.	-99999.99 = Account closed fully paid.	Internal	
Customer management	Vun_Flag	A flag indicating that the customer is vulnerable	Character length 1	V=Vulnerable X = not Vulnerable	Internal	This flag is only populated where the customer is not registered with the VRS[20] but a vulnerability has been identified
....	....	....	....	....	....	....

[20] Vulnerability registration service.

4 Maintenance, audit, and governance

4.1 Maintaining accurate data

In theory, all personal data organisations hold should be accurate and up to date. In practice, there are always some errors or inconsistencies. To comply with GDPR, organisations need to:

- Have robust validation processes in place when they first obtain personal data
- Have mechanisms for identifying and correcting data errors when they come to light
- Have a mechanism for an individual to inform the organisation of errors in their data, so that the organisation can correct it

4.2 Doing something new with data

Whenever an organisation decides to something new with customer data, it needs to assess if the new purpose is compliant under the GDPR. This is additional to the requirement to obtain user's consent if consent has not already been provided.

A Data Protection Impact Assessment (DPIA) is a formal assessment process and should always be undertaken if there is any chance that the processing could be "high risk" for individuals. "High risk" is not explicitly defined by the GDPR, but in relation to consumer lending, the ICO requires organisations to complete a DPIA if they plan to:

- use innovative technology
- use profiling or special category data to decide on access to services
- profile individuals on a large scale
- process biometric data
- process genetic data
- match data or combine datasets from different sources
- collect personal data from a source other than the individual without providing them with a privacy

notice ('invisible processing[21]')

- track individuals' location or behaviour

If any of the above applies to a new use of personal data, a DPIA is required. Any use of Special Category Data (see glossary) is considered high risk, and therefore, a DPIA performed wherever the use of this type of data is proposed.

One example of where a DPIA may be required for a credit union is where the credit union decides that it wants to match all customer records against a new third party fraud database to identify potential fraudsters. They will then carryout checks and potentially close accounts where fraud is found.

A second example is where a lender wants to implement a new system that involves identifying members when they come into branch using facial recognition software. Once identified as a member, staff can then deal with the member, discuss their accounts, and carry out transactions without further verification being required.

A third example is where a lender decides to automate a portion of its underwriting using an AI-based software agent. This would require a DPIA due to being a large scale processing exercise using innovative technology (AI) and due to decisions being undertaken in an entirely automated way.

Minor changes or upgrades to existing processes, or processes that do not result in a "high risk" do not require a DPIA. However, if there is any doubt, then good practice is to undertake a DPIA, with the potential risks being identified and quantified as part of the DPIA process. One role of an organisation's data protection officer (See Section 4.5) is to advise the business if a DPIA is required.

Further information about the DPIA process is available from the ICO website.

4.3 Information about people who are deceased

Information relating to a deceased person does not constitute personal data under GDPR. Therefore, it is not subject to GDPR. Having said this, good practice is to treat information about people who are deceased in a similar manner to living individuals and apply similar data retention policies in case there are any queries or complaints arising from the deceased's estate.

4.4 Audit

An organisation's GDPR compliance, as defined in its data protection policy, should be included as part of the wider audit activities undertaken by the business. This includes an assessment of:

[21] This is a relatively rare situation in regulated industries, relating to cases where, for example, it may not be possible inform someone of processing because you don't have their contact details

- The accuracy of the data that an organisation holds
- The effectiveness of the controls in place to check and validate data, and to correct that data if it is found not to be accurate
- The robustness of the organisations data security procedures
- Compliance with the data retention policy (See Section 5)

Often the audit will include taking random data samples and testing the accuracy of the data against source, through to end point use. For example, testing that the data being used by a DCA matches the data held in the lender's loan application and account management systems.

The data audit may also consider the number and type of customer complaints to identify data quality related issues that have caused complaints to be raised.

4.5 Governance and the Data Protection Officer (DPO)

By its nature, any organisation providing consumer credit products and services will be dealing with considerable amounts of personal data daily. This will often include special category data about health or other vulnerabilities. Therefore, lenders should have a designated Data Protection Officer (DPO). The DPO is responsible for ensuring the organisation's compliance with GDPR and acts as the primary contact with the ICO when needed. This responsibility is delegated by the Board, who have ultimate responsibility for data protection compliance.

The DPO should be a data protection expert[22], who operates independently of individual business functions and has no conflicts of interest. For example, they should not report to the IT director or into another business function that processes personal data. The DPO should report directly to the Board.

The activities DPOs are responsible for include:

- Being the central point of contact for data protection issues. This includes:
  - Staff queries about data protection, and advising on what action is appropriate in given situations
  - Consumer queries, such as subject access requests
  - The ICO
- Maintenance of privacy statements and the data retention policy

[22] Regulation does not define "expert", but the DPO must be someone with considerable professional experience and knowledge of data protection law.

- Maintenance of the data inventory
- Undertaking of regular audit activities to ensure the firm's on-going GDPR compliance
- Reviewing and approving DPIA's when new uses of data are being proposed. This also includes advising the business if a DPIA is required or not
- Providing input to and overseeing staff training

Where data protection issues or data breaches are identified, the DPO has responsibility for reporting these at appropriate internal governance forums (eg the Board or Risk committee) and to the regulator ie the ICO.

For smaller organisations, it is permissible to share a data protection officer, provided that the DPO can fulfil their duties for each organisation. This may be particularly appropriate for some credit unions and CDFIs who they operate similar business models for similar customer groups.

5 Data retention policy

All organisations that hold personal data should have a data retention policy that describes:

- How long different types of data are held
- When data should be deleted
- When data should be retained, but de-personalised (redacted / anonymised)

The data retention policy may be a standalone policy or a sub section within the organisation's broader data protection policy.

The data retention policy sets out the firm's general, high level, approach to data retention. It is used to support the policies applied in each business area, the Data Inventory, privacy notices and any other policies or documentation that refers to data retention.

The data retention policy also applies to physical records as well as electronic ones.

5.1 Depersonalisation (anonymisation and pseudonymisation)

5.1.1 Anonymisation

Personal data is only deemed to be personal data if it can be linked to a specific individual. If data is fully anonymised, then it is no longer classified as personal data and can be used without reference to the GDPR. Fully anonymised means that there is no way to reverse the anonymisation process once it has occurred. It is irreversible.

Anonymisation is commonly applied when organisations need to retain data for analytical and research purposes, but there is no requirement to know who that data relates too. One example of this is found with banks and building societies that need to retain long run data to comply with PRA capital requirements (IRB institutions in particular).

As a minimum, anonymisation requires the removal of names, addresses and dates of birth. However, consideration also needs to be given to any other features of accounts that could, if known, lead to the data being linked to an individual. In particular, where there are two innocuous pieces of information that on their own can't be used to identify someone, but together they could. An example of this is keeping the customer's date of birth and their postcode. Neither on their own will identify a single person[23], but together it is very likely that they would.

More sophisticated anonymization techniques modify or perturb the data in some way. For example, if an organisation wants to know the age profile of its customers historically it needs to retain age/dob information. Therefore, a random number of days (say plus or minus 30 days) is added to each date of birth. The overall age profile across the data won't change significantly, but customers are no longer associated with their true date of birth.

5.1.2 Pseudonymisation

Sometimes, an organisation may create a dataset that contains anonymised personal data, but the dataset has a link, a match key, back to the original data source. This then allows the data to be matched back to individuals if required. This process is referred to as pseudonymisation.

Given the match key allows individuals' data to be identified, pseudonymised data sets continue to be classified as personal data. However, by only including the match key rather than the original data, the data more secure, and hence, reduces the risk of harm in the case of data breaches or unauthorised access.

5.2 Example of a data retention policy

5.2.1 Background

All Welcome Credit Union (AWCU) provides savings accounts and loan products to its members. They operate an industry standard approach of collecting customers' personal details when they apply for membership or a product, and updating these whenever the customer informs them of a change in circumstances. As part of the application process for loans, open banking and credit reference agency data is also obtained.

During their time as a member, the credit union maintains information about the running of the customers' account(s) including their payments, balances, and any arrears. They will obtain an additional credit report for the customer and updated open banking details each time the customer applies for a new product or service. Details about individuals' specific circumstances are maintained as case notes or indicator flags, recording information that customers have provided to help AWCU manage their accounts in line with their requirements. For example, details of vulnerabilities, accessibility requirements, requests for help and so on. Some of this information is classified as special category data.

[23] In general, a single postcode covers about 20 properties, but there are exceptions where a postcode contains just a single residence, and hence, a full postcode could be used to identify some people in a small number of cases.

5.2.2 The Data Retention Policy

All Welcome Credit Union

Data Retention Policy

1. Introduction

At All Welcome Credit Union (AWCU), we are committed to protecting our members' personal data. This Data Retention Policy describes our approach to data retention and the measures we take to ensure that personal data is managed responsibly and in compliance with applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The purpose of this Data Retention Statement is to:

1. Clearly state our data retention practices
2. Ensure that personal data is only retained for as long as necessary
3. Comply with legal and regulatory requirements related to data retention

2. Data Retention Principles

Our data retention practices are guided by the following principles:

- Lawful purpose: We retain personal data only for legitimate business purposes
- Accuracy: We strive to keep personal data accurate, relevant, and up to date
- Minimization: We keep the amount of personal data we maintain to a minimum, where it is necessary for the specified purposes in delivering our services to our members

3. Data Retention Periods

3.1 Member Data

Personal data of credit union members will be retained for as long as the individual is an active member of the credit union. Once a membership ceases, their data will be retained for seven years from the date of account closure. If a customer makes a formal complaint against AWCU during this seven year period, then data will be retained for seven years following resolution of the complaint.

These retention periods are necessary for compliance with financial regulations, audit purposes, and to address any potential legal claims or disputes.

3.2 Employee Data

Employee data, including but not limited to HR records, payroll, and performance evaluations, will normally be retained for 6 years after the employee's employment ends. This retention period allows the credit union to fulfil its legal obligations under tax and employment laws[24], and to address any potential legal claims or disputes. Personal data may be held for longer periods (potentially indefinitely) if a former employee requests that we do so to support them with references beyond 6 years. We keep records of job applications for 3 years from the date of application.

3.3 Marketing Data

Marketing data, including consent records, for direct marketing purposes, will be retained for a maximum of 12 months.

3.4 Extended Data Retention

Occasionally, there may be exceptions where the retention requirement does not fall into the above timescales. For example, data is required to support ongoing investigation by FOS or to support a criminal investigation by the police or other authorities. In these circumstances, the business function that requires the data (see Data Inventory) can submit an exception request to AWCU's Data Protection Officer, which must be approved by the Board prior to the extension being granted.

4. Data Disposal

At the end of the designated retention periods, personal data will be securely disposed of or anonymized to prevent unauthorized access or use. The disposal process will comply with the credit union's security and data protection policies.

5. Data Review / Audit

AWCU will conduct an annual audit of its data assets to ensure they remain accurate, relevant, and up to date. Any data that is no longer necessary will be deleted or anonymized promptly. Where data is found to be inaccurate then the Board will initiate action to correct the identified issue.

6. Training and Awareness

All employees and relevant third parties will be provided with training and awareness programs to ensure they understand their responsibilities in adhering to this data retention policy.

7. Policy Review

This data retention policy will be reviewed annually to ensure ongoing compliance with changes in UK data protection laws and other relevant regulations.

Approved by: [Board or delegated Sub Committee]

Date: [date of approval]

Latest date for next review of this policy [Date of next review]

[24] This period is required to provide confirmation of employment for those seeking employment with FCA regulated firms.

6 Appendices

6.1 Appendix A: glossary of terms used in this document

Term	Description
Credit Reference Agency (also known as a Credit Bureau)	An organisation, licensed under the Consumer Credit Act 1974, to hold information about individuals' repayment behaviour when using credit products such as mortgages, loans, and credit cards. Nearly all UK-based Lending institutions provide details of the balances and arrears status of their customer accounts to one or more of the UK credit reference agencies each month. When a new customer applies for a loan, a lender will purchase a copy of the customer's credit report from the CRA, which details the balances and arrears status of the customers current and previous loan agreements with other lenders. The 3 main credit reference agencies in the UK are Experian, Equifax, and TransUnion (formally CallCredit).
Credit Score	A credit score is a number which provides a holistic view of a customer's creditworthiness based on several different features (characteristics). Typically, these are a mixture of geo-demographics (eg age, occupation, residential status) and financial history (eg number of existing credit agreements, credit card utilisation, defaults, and court judgements). Credit Reference Agencies each provide their own credit scores and the scores differ between agencies due to the different data and methodologies used to create them. Individual lenders often develop their own Credit Score(s), which are tailored to their customer base and may incorporate additional data sources that they have available.
Data Protection Impact Assessment (DIPA)	A process for assessing the impact of new types of processing of personal data where there the processing is deemed to be "High Risk". A firms data protection officer should be able to advise if a process is deemed high risk or not.

Term	Description
Data Protection Policy	An internal policy document covering an organisations use of personal data and detailing how it complies with GDPR. Data retention may form a sub-section of this policy or be a standalone policy that this policy references.
Data Retention Policy	A policy that details the organisations data retention policy. Often a sub-section of the wider data protection policy.
General Data Protection Regulation (GDPR or UK GDPR)	The EU law on data protection that has been adopted into UK law via the UK Data Protection Act 2018. In the UK, GDPR is sometimes referred to as UK GDPR to differentiate it from the EU implementation post Brexit.
Information Commissioner's Office (ICO)	The government body responsible for ensuring organisations comply with the UK implementation of GDPR.
Privacy Notice	A public statement informing individuals about the types of data that an organisation collects and what it does with that information. The notice should also provide details of individuals' rights under GDPR and how long the organisation keeps their data.
Special Category Data	Special Category Data is data that relates to an individual's race or ethical origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning their health, sex life or sexual orientation The presumption is that this type of data needs to be treated with greater care because collecting and using it is more likely to interfere with people's fundamental rights or increase the risk of someone being discriminated against.
Subject Access Request (SAR)	The right under GDPR for a customer to request that an organisation provides details of the information that they hold about them.
Vulnerability Registration Service	The Vulnerability Registration Service ('VRS') is an initiative to help vulnerable individuals protect themselves against the financial, social, and very personal hardship suffered because of debt and financial problems. The service allows people to register that they have a vulnerability. This is then available for financial services organisations to access

Term	Description
	to help them treat customers fairly and meet their obligations under consumer duty.