Document control

Document Title	GDPR Data Audit v0.1		
Version Number	0.1	Author	Selina Tsang
Document status	Approved	Effective date	
Approved by	Tony Brockley	Date approved	23/4/18
Superseded Version		Date of next review	

Version control

Version	Date	Author	Changes
0.1	24/4/2018	S Tsang	Created document

To be reviewed

Section	Last reviewed	Review Due
Data Protection Officer	24/4/2019	24/4/20 [Annually]
LIA	22/5/2019	22/5/20 [Annually]

1.0 Introduction

This document sets forth the expected behaviours of DCU in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a DCU members (i.e. the Data Subject). Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. DCU, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose DCU to complaints, regulatory action, fines and/or reputational damage.

DCU's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all DCU Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

The document was approved by Tony Brockley, CEO of DCU.

2.0 Lawful basis for processing data

In order to process data lawfully under GDPR, DCU has established and documented a lawful basis for processing personal data under the Excel spreadsheet which accompanies this document.

2.1 Consent of the data subject

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. Consent must be some form of clear affirmative action or a positive opt-in, consent cannot be inferred from silence, pre-ticked boxes or inactivity.

Consent is separate from other terms & conditions and is not 'bundled in' with other written agreements or declarations. Data subjects are informed that they have the right to withdraw consent at any time and are provided a simple method for doing so. In addition to the right to be informed, DCU specifically name any third-party controllers (i.e. organisations that wish to use the data for their own purposes) that they intend to share they data with.

The key to reliance on consent for processing is that the collection and maintenance of consent is documented. This includes the evidence of consent – who, when, how, and what you told people.

Where the lawful basis of processing is consent, members may withdraw this consent at any time therefore reliance on consent should be minimised.

DCU's consent checklist

- Freely given
- Specific and granular
- Informed
- Clear, affirmative, unambiguous
- Unbundled
- Easy to withdraw
- Documented

DCU has followed ICO's recommended checklist with regards to consent:

1. Asking for content
☐ We have checked that consent is the most appropriate lawful basis for processing. ☐ We have made the request for consent prominent and separate from our terms and conditions. ☐ We ask people to positively opt in. ☐ We don't use pre-ticked boxes or any other type of default consent. ☐ We use clear, plain language that is easy to understand. ☐ We specify why we want the data and what we're going to do with it. ☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing. ☐ We name our organisation and any third-party controllers who will be relying on the consent. ☐ We tell individuals they can withdraw their consent. ☐ We ensure that individuals can refuse to consent without detriment. ☐ We avoid making consent a precondition of a service. ☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.
2. Recording consent
☐ We keep a record of when and how we got consent from the individual. ☐ We keep a record of exactly what they were told at the time.
3. Managing consent
☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed. ☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents. ☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice. ☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so. ☐ We act on withdrawals of consent as soon as we can. ☐ We don't penalise individuals who wish to withdraw consent.

2.2 Contract

Consent under a contract is when data processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract. DCU has a lawful basis for processing if:

- DCU has a contract with the individual and needs to process their personal data to comply with DCU's obligations under the contract.
- DCU hasn't yet got a contract with the individual, but the individual has asked DCU to do something as a first step (e.g. provide a quote) and DCU needs to process the individual's personal data to do what they ask.

For DCU, this covers all of the information necessary to deal with the member.

2.3 Legal obligation

This basis supports all the information processed for legal obligations such as:

- identity and verification information to comply with anti-money laundering legislation
- tax jurisdiction information for compliance with international tax co-operation legislation
- membership details such as date of enrolment under the Co-operative and Community Benefit Societies Act 2014

2.4 Vital interests

This only applies in life or death situations so it is generally not relevant to DCU's data processing.

2.5 Public task

This is generally not relevant for DCU's data processing but it can apply if DCU exercises official authority or carries out tasks in the public interest, such as research using member data in the public interest.

2.6 Legitimate interests

This lawful basis is likely to be most appropriate where you use people's data in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing. A Legitimate Interests Assessment (LIA) was undertaken and diarised for regular review.

3.0 Individual Rights

Members' rights under GDPR are:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automating decision-making and profiling

3.1 The right to be informed

DCU provides individuals with information including: DCU's purposes for processing their personal data, retention periods for that personal data, and who it will be shared with in a the privacy notice. The privacy notice is provided to individuals at the time their personal data was collected from them (e.g. completing application forms, loan applications).

3.2 The right of access

DCU will provide a copy of a member's information free of charge. However, DCU may charge a reasonable fee (i.e. accounting for the costs of administration) for further copies of the same information.

Where requests are manifestly unfounded or excessive, particularly when these are repetitive requests, DCU may:

- charge a reasonable fee (i.e. related to the costs of administration); or
- refuse to respond to the request

Where DCU refuse to respond to a request, DCU will explain why to the individual and inform them of their right to complain to the ICO and to a judicial remedy. This explanation should be made without undue delay and within one month at the latest.

DCU will comply with the subject access request without undue delay, and within one month. It is possible to extend the period of compliance by a further two months where requests are particularly complex or numerous, where this is the case, DCU will inform the individual within one month of receipt and explain the reason the extension is necessary.

If it is provided electronically, DCU will provide it in a PDF format.

DCU will verify the identity of the person making the request using 'reasonable means' and may use their standard verification for account access.

DCU has followed ICO's recommended checklist with regards to an individual's right to access:

Preparing for subject access requests

☐ We know how to recognise a subject access request and we understand when the right of access applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

☐ We understand the nature of the supplementary information we need to provide in response to a subject access request.

Complying with subject access requests

☐ We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.

☐ We understand what we need to consider if a request includes information about others.

3.3 The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Where personal data has been disclosed to third parties, DCU must inform them of the rectification where possible. DCU should also inform the individual which third parties you have disclosed their data to where appropriate.

DCU will respond in one month, which can be extended by two months where requests are particularly complex or numerous. You must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where DCU decides not to take action in response to a request for rectification, DCU must explain why to the individual and inform them of their right to complain to the ICO and to a judicial remedy.

DCU has followed ICO's recommended checklist with regards to an individual's right to rectification:

Preparing for requests for rectification ☐ We know how to recognise a request for rectification and we understand when this right applies. ☐ We have a policy for how to record requests we receive verbally. ☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so. Complying with requests for rectification ☐ We have processes in place to ensure that we respond to a request for rectification without undue delay and within one month of receipt. ☐ We are aware of the circumstances when we can extend the time limit to respond to a request. ☐ We have appropriate systems to rectify or complete information, or provide a supplementary statement. ☐ We have procedures in place to inform any recipients if we rectify any data we have shared with them.

3.4 The right to erasure

Also known as the 'right to be forgotten' the right of erasure enables individuals to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

This applies in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent, where the grounds of processing is based on consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR)
- The personal data has to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services (online services) to a child

3.4.1 Exemptions (refusing the request)

Credit unions are able to refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- The exercise of defence of legal claims
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- To exercise the right of freedom of expression and information
- Archiving purposes in the public interest, scientific research, historical research, or statistical purposes

Where information has been made available to third parties you must inform them of the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Credit unions have one month to respond to the erasure request. This can be extended by two months if requests are particularly complex or numerous.

Where the credit union decides not to take action in response to a request for erasure, it must explain why to the individual and inform them of their right to complain to the ICO and to a judicial remedy.

DCU has followed ICO's recommended checklist with regards to an individual's right to erasure:

Preparing for requests for erasure

☐ We know how to recognise a request for erasure and we understand when the right applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for erasure

☐ We have processes in place to ensure that we respond to a request for erasure without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.

☐ We have procedures in place to inform any recipients if we erase any data we have shared with them.

☐ We have appropriate methods in place to erase information.

3.5 The right to restrict processing

When processing is restricted, DCU is permitted to store the personal data but not further process it. DCU will retain just enough information to ensure that the restriction is respected in future and inform any third parties about the restriction on the personal data unless it is disproportionate to do so.

This applies in the following circumstances:

- Where an individual contests the accuracy of the personal data, DCU will restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the purpose of legitimate interests), and DCU are considering whether the legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If DCU no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

DCU has one month to respond to the restriction request. This can be extended by two months if requests are particularly complex or numerous.

Where DCU decides not to take action in response to a request for the restriction, DCU must explain why to the individual and inform them of their right to complain to the ICO and to a judicial remedy.

DCU has followed ICO's recommended checklist with regards to an individual's right to restrict processing:

Preparing for requests for restriction

☐ We know how to recognise a request for restriction and we understand when the right applies.

☐ We have a policy in place for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for restriction

☐ We have processes in place to ensure that we respond to a request for restriction without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We have appropriate methods in place to restrict the processing of personal data on our systems.

☐ We have appropriate methods in place to indicate on our systems that further processing has been restricted.

☐ We understand the circumstances when we can process personal data that has been restricted.

☐ We have procedures in place to inform any recipients if we restrict any data we have shared with them.

☐ We understand that we need to tell individuals before we lift a restriction on processing.

3.6 The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This should be proved in a structured, commonly used and machine-readable format e.g. CSV files. This enables other organisations to use the data and should be provided free of charge.

This data is not limited to information provided directly by the individual (e.g. through an online form) but also extends to data generated by the activity of that individual.

This applies where:

- The individual supplied the data to the controller
- The processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means

DCU will respond without undue delay, and within one month. This can be extended by two months where the request is complex or DCU receive a number of requests. DCU must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where DCU decides not to take action in response to a request, you must explain why to the individual, informing them of their right to complain to the ICO and to a judicial remedy without undue delay and at the latest within one month.

DCU has followed ICO's recommended checklist with regards to an individual's right to data portability:

Preparing for requests for data portability

☐ We know how to recognise a request for data portability and we understand when the right applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for data portability

☐ We can transmit personal data in structured, commonly used and machine readable formats.

☐ We use secure methods to transmit personal data.

☐ We have processes in place to ensure that we respond to a request for data portability without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

3.7 The right to object

Individuals have the right to object to certain kinds of processing such as:

- Processing based on legitimate interests
- Direct marketing (including profiling); and
- Processes for the purposes of scientific/historical research and statistics
- Performance of a task in the public interest/exercise of official authority (including profiling)

Where these processing activities are carried out online, DCU offers a way for individuals to object online.

Processing personal data for direct marketing purpose

DCU will stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse. This must be dealt with free of charge.

Processing based on legitimate interests

DCU will stop processing the personal data unless one of the following applies:

- DCU can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
- The establishment, exercise or defence of legal claims;
- The individual does not have an objection on grounds relating to his or her particular situation

DCU will inform individuals of their right to object at the point of first communication and in your privacy notice. This must be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

DCU will respond without undue delay and within one month. This can be extended by two months where the request is complex or you receive a number of requests. You must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where DCU decides not to take action in response to a request for erasure, it must explain why to the individual and inform them of their right to complain to the ICO and to a judicial remedy.

DCU has followed ICO's recommended checklist with regards to an individual's right to object:

Preparing for objections to processing

☐ We know how to recognise an objection and we understand when the right applies.

☐ We have a policy in place for how to record objections we receive verbally.

☐ We understand when we can refuse an objection and are aware of the information we need to provide to individuals when we do so.

☐ We have clear information in our privacy notice about individuals' right to object, which is presented separately from other information on their rights.

☐ We understand when we need to inform individuals of their right to object in addition to including it in our privacy notice.

Complying with requests which object to processing

☐ We have processes in place to ensure that we respond to an objection without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to an objection.

☐ We have appropriate methods in place to erase, suppress or otherwise cease processing personal data.

4.0 Information audit

An information audit was undertaken to systematically check for compliance with data protection regulations to ensure:

- Data collected is obtained on a legitimate and lawful basis
- Information is accurate, complete, up-to-date, relevant and not excessive
- Data is stored securely, whilst use and access of systems containing personal data is controlled and limited
- Data is processed appropriately and in line with data subjects' expectations
- Compliance with individual's rights such as subject access rights and right to be informed
- Data is shared securely and appropriately with third parties, and individuals are informed of the data sharing
- Data is not retained indefinitely, and controls are put in place for the deletion of the data

This audit process undertaken consists of these elements:

1. Data Collection
2. Data Storage
3. Data Processing
4. Data Sharing
5. Data Maintenance
6. Data Destruction

This document summarises the work and policy regarding these elements and the actual audit is presented in the Excel spreadsheet which accompanies this document.

4.1 Data collection

This section of the audit reviews the ways that data is obtained or received by DCU such as all forms, notes made when dealing with members, e-mails, and beneficiaries. Data is categorised into either personal or sensitive data and evaluated against these questions:

- What personal data is collected?
- What categories of personal data are collected?
- What will the data be used for, is this lawful?
- Is all of the data necessary?
- Is any of the information sensitive personal data?
- Is a privacy policy provided to individuals when the information is collected?

4.1.1 Personal/sensitive data definition

Personal data is defined under the GDPR as any information relating to an identified or identifiable natural person (data subject). Identifiable (as opposed to identified) natural persons are data subjects which cannot be directly identified but can instead be indirectly identified from one or more pieces of information relating to that person.

Whether or not an individual can be identified from data depends on the context, for example, by itself the name John Smith may not always be personal data due to how many individuals have that name. However, where the name is combined with other information – such as an address, place of work, or telephone number – this will usually be sufficient to clearly identify one individual.

This means that any information that can be linked to a specific individual is personal data and can include a wide variety of data items from basic contact details to IP addresses in the right context.

Examples of personal data:

- Name
- Address
- Date of Birth
- Marital Status
- Financial Transactions
- Photographs / Video
- IP Addresses
- Mobile ID
- Notes relating to a person
- Recorded phone calls
- National insurance number
- Sensitive personal data

Sensitive personal data is data that has a higher potential to cause harm to a data subject and is defined under the GDPR as data revealing the following:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs,

- Trade union membership
- Data concerning health
- Data concerning sex life and sexual orientation
- Genetic; and
- Biometric data (includes finger prints, eye and voice recognition)

4.2 Data storage

A key component of the audit is going to be assessing how and where all of DCU's data is stored. Data will be stored either on DCU's premises or remotely by a third party, it may be stored in a number of different formats. DCU's methods of storing data was reviewed and audited.

4.3 Data processing

Credit unions process data for a variety of different purposes which prescribes what data is collected, how it is shared, and how long it is retained for. The processing should be for specific, explicit and specified purposes. Typical processing activities include:

- Membership applications
- Loan processing
- Identification for AML compliance
- Processing transactions (deposits, transfers, dividend)
- Dealing with a complaint
- Direct marketing
- Communications with members
- Administering ELDS
- Equal opportunities and social impact assessments

The audit confirms that DCU can ensure that they process data in line with the reasons given to the member when the member provided the information. However, it is possible to process for new purposes as set out below.

4.3.1 Processing for new purposes

Credit unions can process information for a new purpose providing that they consider whether the new purpose is compatible with the original purpose taking into account the following factors:

- Any link between the original purpose and the new purpose
- The context in which the data has been collected
- The nature of the personal data and whether sensitive personal data is affected
- The possible consequences of the new purpose of processing for the data subjects
- The existence of appropriate safeguards (e.g. encryption or pseudonymisation)

4.4 Data sharing

DCU will share some data with third parties and will need to ensure that all third parties can be trusted and that the sharing mechanism is secure.

Third parties that DCU may share personal data with include:

- Credit reference agencies

- Identification / Verification company & Know Your Customer Services
- PEPs and Sanctions service provider
- Website provider
- Data back-up provider
- Financial Services Compensation Scheme
- National Crime Agency
- Mailing solution providers
- HM Revenue and Customs
- Banking platform provider
- Customer Relationship Management system

DCU reviewed all the third parties who it shares data with to ensure that they were trusted and that data was secure.

4.5 Data Maintenance

One of the principles of GDPR is that personal information should be accurate and kept up-to-date where necessary. DCU will continually update the information on their members as they are informed of changes to their personal data and consider providing further prompting and mechanisms for members self-maintain their personal information.

Where DCU discovers new information about a member, this may need to be passed on to third parties as appropriate.

4.6 Data Destruction

After a certain amount of time after members leave, or where information relating to a member is no longer needed, DCU will need to erase personal information in line with a retention policy. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Even though DCU may no longer need the personal data, DCU ensures that it is held securely. Where DCU decides to delete data it should delete all instances of that data and erase any backups that have been made. Where the data has been provided to third parties, DCU should ensure that these are also adhering to a retention schedule.

The retention policy was updated and data destruction procedure was confirmed which considered third parties and the deletion of all instances of data, such as back-ups or paper copies.

5.0 Data Protection Officer – Source: ABCUL

"A Data Protection Officer (DPO) is responsible for monitoring and advising firms on GDPR compliance. This person can be a member of staff, or could be external and shared between different firms. The DPO is required to have certain professional qualities and a certain level of independence and resource in order to perform the role. Credit unions must appoint a DPO if their core activities require:

- *Regular and* systemic monitoring of individuals on a large scale; or
- Processing on a large scale of special categories of data or personal data relating to criminal convictions or offences

Large scale – The GDPR does not define what constitutes large scale processing and instead the EU Working Party 29 guidance suggests the following factors are considered when determining whether processing is large scale or not:

- The number of data subjects – either as a specific number or percentage of a population
- The volume of data and/or range of different data items being processed
- The duration or permanence of the data processing activity
- The geographical extent of the processing activity

Examples of large scale processing cited in the guidance:

- Processing of patient data in a hospital
- Processing of customer data in an insurance company or a bank
- Processing a personal data for behaviour advertising in by a search engine

Examples of processing that are not considered large scale:

- Processing of patient data by an individual physician
- Processing of personal data relating to criminal offences by an individual lawyer

The working party guidance acknowledges that there is a "large grey zone in between these extremes" i.e. the difference between the number of people an individual practitioner may serve and a relatively large organisation such as a hospital or bank.

If a credit union decides it does not need a DPO it should record the justification behind its decision and review this decision periodically and when its data processing changes significantly e.g. begins to process more sensitive information such as health records.

Credit unions may appoint a DPO voluntarily, however, that person should meet the same standards as a DPO required by the GDPR. Persons who do not meet these requirements but otherwise perform data protection duties should not be given the job title of 'Data Protection Officer"

DCU has decided not to employ a DPO. DCU does not believe from these definitions that it processes a 'large scale' of data. The percentage of population is only c.7,500 members from the whole of the North East region. This will be reviewed annually unless DCU begins to process more sensitive information.