SCVO CREDIT UNION

DATA PROTECTION POLICY

MAY 2018

Contents

1. Introduction

SCVO Credit Union holds personal data about our employees, members, clients, and other individuals for a variety of business purposes.

This policy sets out how SCVO Credit Union seeks to protect personal data and ensure that Directors, Officers, Volunteers and Staff understand the rules governing their use of personal data to which they have access in the course of their duties. In particular, this policy requires staff to ensure that the Data Protection Officer be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2. Key Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, savings loans and business development purposes. *Business purposes include the following:* • *Compliance with our legal, regulatory and corporate governance obligations and good practice* • *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* • *Ensuring business policies are adhered to (such as policies covering email and internet use)* • *Operational reasons, such as recording transactions, training and ensuring the confidentiality of commercially sensitive information, credit scoring and checking member details* • *Investigating complaints* • *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* • *Marketing our business* • *Improving services*

Personal data	Information relating to identifiable individuals, who will be credit union members, staff, payroll deduction clients, suppliers and marketing contacts. *Personal data we gather may include: individuals' contact details, financial details, For Hr Credit Union purposes details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Sensitive personal data	*Any use of sensitive personal data will be strictly controlled in accordance with this policy. The credit union will not hold any sensitive data for any our members*

Data Processor	A processor is responsible for processing personal data on behalf of a controller. As processors, the GDPR places specific legal obligations on the Credit Union; for example, we are required to maintain records of personal data for

	processing activities (member transactions). As data processors we will have legal liability if we are responsible for a breach. SCVO Credit Union processes data on behalf of payroll customers.

Data Controller	SCVO Credit Union are the data controllers and we will determine the purposes and means of processing personal data The Credit Union as a Controllers, we are not relieved of our obligations where a processor is involved – the GDPR places further obligations to ensure our contracts with processors comply with the GDPR. *(The GDPR applies to 'controllers' and 'processors).* SCVO Credit Union will determine the purpose and means of processing member data for our payroll deduction, direct debt and BACS collection schemes. Employers who submit employee deductions are also the Processors.

3. Scope

This policy applies to all Directors, Officers, Volunteers and Staff. All must be familiar with this policy and comply with its terms.

SCVO Credit Union may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to all Directors before being adopted.

Who is responsible for this policy?

Responsibility for adhering to good data protection practices is the responsibility of all officers, staff and agents of SCVO Credit Union. Corporate responsibility for the maintenance and enforcement of the Data Protection Policy across SCVO Credit Union lies at Director Level.

4. Our Procedures

Fair and lawful processing

SCVO Credit Union will process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we will not process personal data unless the individual whose details we are processing has consented to this happening.

Data protection Officer Responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by SCVO Credit Union.
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities IT:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Ensure that staff only use approved systems for the storage and transfer of data
- Coordinating with the IAO to ensure that appropriate technical and organisational solutions are in place.

Responsibilities for Marketing:

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the Data Protection Officer to ensure all marketing initiatives adhere to data protection laws and SCVO Credit Union Data Protection Policy

The processing of all data MUST be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

5. Privacy Notices

Where data is collected a Privacy Notice to individuals MUST be displayed, this should be clear and unambiguous. All SCVO Credit Union Privacy Notices MUST contain the following as at an absolute minimum:

- Set out the purpose**s** for which we hold personal data on customers and employees
- Inform customers have a right of access to the personal data that we hold about them
- How long the information will be held.
- Provide information on how they can exercise their right to stop data being processed.

If sharing with a 3rd party (e.g. government agency) is occurring:

- Clearly explain what information is being shared and with who.

The Credit Unions privacy notices has included all points of data collection, both digital and non-digital.

Our Privacy Notice Checklist

☐ What information is being collected?
☐ Who is collecting it?
☐ How is it collected?
☐ Why is it being collected?
☐ How will it be used?
☐ Who will it be shared with?
☐ Identity and contact details of any data controllers:
☐ Retention period

SCVO Credit Union will be transparent and providing accessible information to individuals about how we will use their personal data.

6. Consent

The data that we collect will be subject to active consent by the individual. This consent can be revoked at any time.

Example

Email Newsletter: If a member no longer wishes to receive our marketing communication we will stop immediately. We will record their email and date unsubscribed, to avoid adding them in future. However, all other personal information no longer required, will be removed.

Where data must is maintained for a legal or compliance requirement no consent is required, however this will be carefully checked and only the minimal data required will be kept to fulfil those obligations. Once the statutory time limit has passed the data should be removed.

7. Conditions for processing

SCVO Credit Union will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented and recorded (e.g. in Project Documentation). All staff that is responsible for processing personal data MUST be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Conditions of processing checklist:

☐ We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.
☐ We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
☐ We have documented our decision on which lawful basis applies to help us demonstrate compliance.
☐ We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

8. Justification for personal data

SCVO Credit Union will process personal data in compliance with all six data protection principles:

Lawfulness, fairness and transparency:

- Transparency: We will inform subject (memerbs) what data processing will be done.
- Fair: What is processed must match up with how it has been described
- Lawful: Processing must meet the tests described in GDPR

Purpose limitations:
Personal data can only be obtained for specified, explicit and legitimate. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

Data minimisation:
Data collected on a subject should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

No more than the minimum amount of data should be kept for specific processing. SCVO Credit Union will never collect or 'horde' data just because it may be useful in the future.

Accuracy:
Data must be accurate and where necessary kept up to date. Baselining ensures good protection and protection against identity theft.

Storage limitations:
Personal data is kept in a form which permits identification of data subjects for no longer than necessary. Data no longer required should be removed. Managers MUST maintain a schedule of data in their departments (Standard SCVO Data Mapping Template).

Integrity and confidentiality:

SCVO Credit Union processors will handle data in a manner ensuring appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage.

9. Data portability

Upon request, a data subject has the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Any such requests must be passed to our Data Protection Officer without any delay.

Sensitive personal data

In member cases SCVO Credit Union will not process sensitive personal data unless without the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

SCVO Credit Union will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and rectify at source without undue delay.

10.Personal data as employees of SCVO Credit Union

We will take reasonable steps to ensure that personal data SCVO Credit Union holds about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Named Employer Directors so that they can update your records.

11. Data security

Keeping personal data secure against loss or misuse.

Where other organisations process personal data as a service on our behalf, the Data Protection officer will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations (Payroll deduction employers).

Data Protection officer must be aware before any passing of sensitive data to a third party, either by electronic, post or voice recording.

Storing personal and sensitive data securely

- In cases when personal/sensitive data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed personal/sensitive data should be shredded when it is no longer needed.
- Personal/sensitive data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a Password Manager to create and store their passwords . *A notebook is not a secure password manager!*
- Personal/sensitive data must not be stored on portable memory unless there is absolutely no alternative. Where there is no alternative, it MUST be locked away securely when they are not being used and MUST be encrypted. Further advice can be obtained from ithelpdesk@scvo.org.uk
- The Data Protection officer must approve any cloud[1] used to store personal/sensitive data.
- The use of alternative cloud storage for personal/sensitive data is expressly forbidden.
- Personal/sensitive data should be regularly backed up in line with the company's backup procedures.
- Personal/sensitive data should never be saved directly to mobile devices such as laptops, tablets or smartphones where the devices are not running approved encryption technologies.

12. Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

13. Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can

[1] In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. Office 365 is an example of cloud computing.

only be refused if an exemption applies (e.g. there is a need to maintain the data to fulfil a contractual, legal or regulatory obligation).

14. Transferring data internationally

There are restrictions on international transfers of personal data. You MUST not transfer personal data anywhere outside the EEA without first consulting the Data Protection officer

15. Subject access requests

Please note that under the General Data Protection Regulation (**GDPR**) (Regulation (EU) 2016/679), individuals are entitled, subject to certain exceptions, to request access to information held about them.

If we receive a subject access request this will be dealt with immediately and under GDPR SCVO Credit Union will respond to such requests in one month.

In order to service Subject Access Requests it is vital that only approved solutions are used to store personal data (see 'Storing data securely').

Please contact the Data Protection officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law

16. Processing data in accordance with the individual's rights

The Credit Union will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Data Protection officer about any such request.

The Credit Union will not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed and consent has been **freely** given and recorded. .

17. Training

All staff have received training on this policy. New starters will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house online seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.
- Cyber and e-security.

18. Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The IAO and Head of IT will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Staff must become familiar with this policy and include privacy and good data protection practices as core within any new project design or material change to an existing project.

19. Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

The audits shall be reviewed annually by the Data Protection officer and noted with a review date.

It is the responsibility the all staff to provide accurate information during these audits. Managers MUST alert the Data Protection Officer if there has been, or is planned to be, a material change in processing.

This will be surfaced onto SCVO Credit Union as an at Risk Register as a single item, 'Personal/Sensitive Data'.

20. Reporting breaches

All Directors, Officers, Volunteers and Staff have an obligation to report actual or suspected data protection compliance failures. This allows us to:

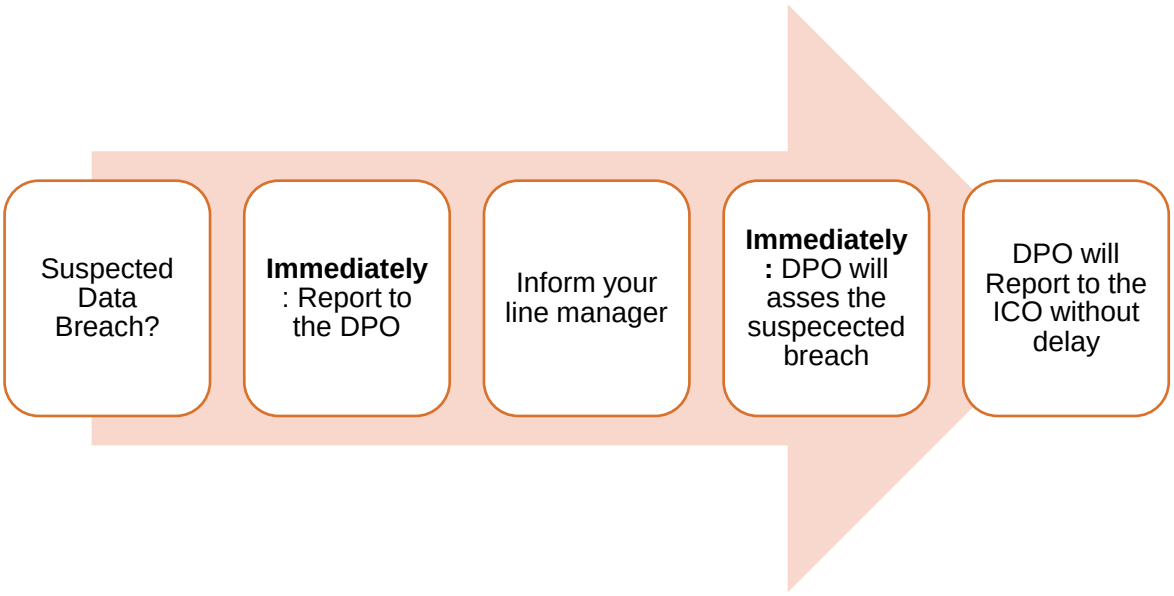
- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures
- Minimise the damage done to the individual

Examples of breaches

- access by an unauthorised third party to personal data;
- deliberate or accidental action (or inaction);
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.
- leaving a file on a train.

Where a breach has occurred, or is suspected to have occurred, the Data protection Officer must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

21. SCVO Credit Union Staff Reporting Procedure:



ICO Report Template (IAO Use Only):

Nature of the personal data breach:
The categories and approximate number of individuals concerned and approximate number of personal data records concerned:
The name and contact details of the Data Protection Officer:
Description of the likely consequences of the personal data breach:
Description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects:

Report Via: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

22. Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the SCVO Credit Union at risk. The importance of this policy means that failure to comply with any reporting requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer