Sparcollective

Data Protection & Information Security Handbook

The Data Protection Officer for SPARCollective is: Scott James McMillan; however data protection and information security is the responsibility of everyone at SPARCollective.

History of this Handbook
Document initially drafted June-August 2020.
Reviewed and Revised August 2020.
Discussed at Sparcollective CIC Board Meetings 11 August, 20 August, 27 August 2020.
Approved pending final review and proof reading at meeting of 27/8/2020.
Accepted, finalised and published: 28/8/2020.

To be reviewed annually.

Introduction to the regulations

General Data Protection Regulations

The European Union legislation known as the General Data Protection Regulations (GDPR) is enforced from 25th May 2018. This handbook, associated policies and procedures are all designed to ensure compliance with these regulations.

Controllers and Processors

SPARCollective (otherwise known as SPARC or "Scottish Prisoner Advocacy Research Collective") is the controller for data collected relating to its services and activities.

A processor is an individual responsible for processing personal data on behalf of SPARCollective– for example, a member of our staff.

Both processors and controllers are legally responsible for their handling of personal data, and individual processors can have legal liability for breaches, as well as there being legal responsibilities placed on data controllers.

Personal Data

The GDPR applies to "personal data", meaning any information relating to an identifiable person who can be directly or indirectly identified by that information. A range of personal identifiers can therefore constitute personal data, including name, an ID number, an address etc.

The GDPR applies to both manual and IT-based filing systems where personal data are recorded.

Special Categories of Data

Additionally, there are special categories of data which require special measures of risk control to be in place when handled. These are:

- biometric information (body measurements used as identification)
- genetic information
- racial / ethnic origin
- political opinion
- religious belief
- membership of trade union
- physical or mental health condition
- sexual orientation / sexual life
- gender

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing, and we will apply these given the nature of our CIC's community.

Principles of Data Processing

The principles of data protection set out in the GDPR legislation allow organisations to consider how they handle the personal data of others.

Data must be:

- processed lawfully, fairly and transparently
- collected for a specific purpose and used for nothing other than that
- enough, but no more than is needed to do what is required with the information
- accurate and kept updated, with inaccurate data erased / rectified without delay
- kept in a form where people can be identified for no longer than is necessary
- archived appropriately for purposes of public interest, statistical purposes
- archived in such a way that the rights and freedoms of individuals are upheld
- processed securely and lawfully, protected from loss destruction or damage

There is an additional duty for responsibility and evidence of compliance with the principles. SPARCollective ensures compliance through the procedures and policies in place relating to data processing and information security.

Individuals Rights and Freedoms

GDPR includes rights for individuals – this part of the handbook explains these rights and our standard organisational response to these when processing data.

The right to be informed

The right to be informed means that we have an obligation to "fairly process" information. We do this through our privacy notice. This emphasises the need for transparency over how we will use your personal data. Our Privacy Notices can be found at https://scottishprisoneradvocacy.com/ .

The right of access

At any point an individual can make a request relating to their data and SPARCollective will provide a response (within 1 month). Individuals can access their data to ensure that it is being processed lawfully by our organisation. Given the timescales for

response, a member of SPARCollective receiving a request for access from an individual should pass this to the Data Protection Officer within 5 days. This allows for maximum time to collate and prepare information for the enquirer.

The right to erasure / rectification

The right to erasure is also known as “the right to be forgotten”. The broad principle underpinning this right is to enable the individual to ask for the removal of data relating to them where there is no compelling reason for its continued use.

Individuals must be informed that the erasure of their information will result in the inability of SPARCollective to communicate with them, or – where this is also requested for deletion – use the information that they have provided us with in our advocacy and policy work. Requests will be actioned within 30 days of being received.

Additionally, individuals are entitled to have their personal data rectified if it is inaccurate or incomplete. It’s vital that we maintain a clear trail if information is shared with other agencies and therefore must ensure that, as far as possible, any notification of changes is passed on also.

Any request for rectification must be responded to within 1 month and should be passed on to the Data Protection Officer once received, enabling them to co-ordinate the trail of changes to be made.

The right to restrict processing

Individuals can object to SPARC processing their data. This means that records can be stored but must not be used in any way, for example, in reports or for communications. This right may not always be relevant, as SPARCollective may be required to process information to comply with a contractual obligation.

The right to data portability

Under the GDPR, you have a right to data portability. This means that you have the right to receive the personal data we hold on you in a structured way, and to request that this data is transmitted directly to another secure data controller. We will respond to all data portability requests within one month.

The right to object

Individuals can object to their data being used for certain activities like marketing or research. As with the application of other rights, this can hinder the delivery of service to individuals.

The right not to be subject to automated decision-making, including profiling.

Automated decisions and profiling are used for marketing-based organisations. SPARCollective does not use personal data for such purposes.

<u>Individual Responsibilities</u>

All individuals handling data on behalf of SPARCollective have a responsibility for compliance with these procedures. An overview of responsibilities is contained within the organisation’s Data Protection & Information Security Policy.

The consequences of getting data processing wrong are substantial. Not only can it erode trust in our organisation and damage our reputation, but it may also leave SPARCollective and those who have inappropriately handled data open to substantial fines under the GDPR. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of €20 million or 4% of the organisation's turnover – whichever is higher.

Where staff are unable to access emails for longer than 3 working days, they should amend their out of office notification to ensure that individuals seeking to engage with the organisation are able to access the Data Protection Officer directly.

"*Requests relating to data protection should be sent to our Data Protection Officer by email to: scot.prisoner.advocacy.mydata@gmail.com*

Where the Data Protection Officer is not able to respond to enquiries within the stated timeframes, due to extended leave, sickness or any other legitimate reason, then an appropriate person within the organisation must be afforded delegated authority and responsibility to handle enquiries in their absence.

Key Activities and Data Protection Procedures

Employee Administration

This section covers data processing activities relating to how SPARCollective handles employee data for administration purposes.

Recruitment

Potential employees' personal data can be collected as long as the people are aware their data is being recorded and retained. It is imperative that the data collected about potential employees is not excessive – only what is needed – and that it is stored securely and not shared with anyone who has no need to see it. A retention period should be established for this information and once this has elapsed the information should be disposed of securely (deleted from a computer or shredded if manually kept).

Employee Records

When starting employment, employees sign a contract which provides consent to process personal information, sensitive personal information and transferring the data in the delivery of services such as payroll, insurances, and for advice. A retention period of 5 years after employment with SPARCollective ends has been set, after which ANY information should be disposed of securely (deleted from a computer or shredded if manually kept). Employees have the responsibility to ensure that their data remains up to date.

Contact Administration

This section covers data processing activities relating to how SPARCollective handles the data of people who make contact with us, especially (but not exclusively) those who contact us with information to inform our policy and advocacy work.

Contact Data Set

SPARCollective holds and handles some personal data about the people who make contact with us. This information can include: name, contact details (e.g. email address or twitter handle) and information about problems they may face or intelligence to inform our policy and advocacy work. This may implicitly or explicitly include information related to criminal convictions and/or the prisons where someone (or their family member) has resided.

This information is stored on the email and social media accounts through which the person has communicated. All of these accounts are password protected, and the passwords are known only to SPARC directors and members.

Information and intelligence given to support our policy and advocacy work may also be stored in anonymised form in a password protected document. On some occasions it may be necessary to temporarily store this anonymised information on the personal computers of SPARCollective staff.

All SPARCollective directors and staff accessing data will have read and agreed to this Data Protection policy and associated documents.

If SPARCollective wish to use client data for any purpose other than what has initially been declared, then permission must once again be sought from the client to enable this to happen

Data Cleansing

This is a crucial activity in an organisation with multiple contract-based activity undertaken across a number of business streams. It is vital that SPARCollective cleanses its data regularly.

Communications

Contacting people via email or text will require specific consent from them. The ICO has stated that all email addresses are classed as personal data; it is therefore essential that when bulk communicating with people, that the following provisions are made:

- individuals who have opted out of mailings are not included in mailings
- the blind carbon copy (Bcc) function of emails is used
- if a person states they no longer wish to be contacted via email, their details are removed from all mailing lists / distribution lists
- an option to unsubscribe to similar communications is added to the bottom of the message when sent

Research and Insights

This section covers data processing activities relating to how SPARCollective undertakes research activities.

Surveys etc. will be undertaken by consent. Records of the views of individuals will be considered personal data, unless anonymised.

Data published may not identify any individual without their explicit consent, however anonymised data from all datasets may be processed and published for statistical / management information purposes. Such data should be stored securely and deleted at the appropriate point after no longer used.

Service Administration

This section covers data processing activities relating to how SPARCollective delivers administration of services for clients, suppliers, contractors and visitors. This data can include:

- bank account details for the purposes of making payments
- Drivers details for insurance purposes
- Events customers / booking information for the purposes of ticket management
- Retail customers for the purposes of fulfilment, delivery and order management

Third Party Data

Where SPARCollective uses Third Party data, there must be a declaration of its use to the individual whose data is being processed. This must be delivered within 1 month of obtaining the data, at the point of first communication or prior to disclosure to other parties. Should the third party notify SPARCollective, or SPARCollective become aware of any errors in the data, this must be rectified within one month of notification.

At this point in time, SPARCollective does not possess, seek to acquire or handle Third Party data, but should this change, this guidance applies.

Information Security Procedures

Data Storage

Hard Copies, file notes, incoming and outgoing correspondence

SPARCollective has a duty to ensure that data is held securely. Provisions that directors and/or staff must consider putting in place include:

- Lockable filing cabinets
- A clear desk policy
- Secure storage for archived files
- Secure destruction – shredder or effective confidential waste bin

Electronic data

The same requirements apply to electronically held data. Provisions that staff must consider putting in place include:

- Use storage on the company server
- Password protection on all files that include personal data
- Controlled access to systems
- Updates as required to antivirus and malware systems
- Adequate firewalls
- Secure destruction of IT systems

Disposing of IT equipment

Even if you think you have deleted data from your computer, it is likely remaining in some form. Disposing of IT equipment securely is essential. SPARCollective must

ensure that they have sufficient support to ensure that this happens across the organisation.

Email Security

SPARCollective uses one shared email address, which can be accessed by all the directors and staff.

The following steps should be taken to ensure the security of email content:

- Consider whether the content of the email should be encrypted, or password protected. If sending a spreadsheet with personal data, this must be password protected and the password sent in a separate email
- If you want to send an email to a recipient without revealing their address to other recipients, ensure that the Bcc function is used, not carbon copy (cc). When cc is used, all other addresses can see who the email was sent to.

Emails containing any personal information (including names or email address) should not be forwarded on to other email addresses, including personal or other emails belonging to SPARCollective directors.

Information Security Breaches

An information security breach means a situation whereby the loss, damage, destruction, alteration, unauthorised disclosure of or access to personal data. This means that a breach is more than just losing personal data.

A data security breach can happen for a number of reasons:

- Loss or theft of equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking attack
- Deception of the organisation through “blagging” offences

Detecting Data Breaches

Detecting a data breach or the potential of a data breach can happen in a variety of ways. All Data Breaches must be notified to the Data Protection Officer within 24 hours. The table below outlines methods of detection and processes for handling them.

Detection Method	**Action for Potential Breach**	**Action for Actual Breach**
Employee or director detection	If you think you have identified a potential breach in data security, you must immediately inform the Data Protection Officer. They may immediately cease processing the	Immediately report to the Data Protection Officer and / or line manager. Isolate potential for any further breach where

	data until the breach is resolved, based on an assessment of the risk to individual privacy	possible. Management will follow appropriate procedures outlined within this document
Accidental Breach (i.e. loss of laptop)	If there is a high likelihood of this breach happening, you should immediately adjust your processes and procedures to reduce this likelihood. Always ensure that data is secured and encrypted. Consult the Data Protection Officer or line manager where appropriate	Immediately report to the Data Protection Officer and / or line manager. Isolate potential for any further breach where possible. Management will follow appropriate procedures outlined within this document
Detection Method	**Action for Potential Breach**	**Action for Actual Breach**
Audit or Assessment	SPARCollective will conduct regular audits of its physical and electronic information systems. These may highlight weaknesses in the organisation. These should be responded to, according to advice from the Data Protection Officer, in a timely manner to ensure the data privacy of individuals	Immediately report to the Data Protection Officer and / or line manager. Isolate potential for any further breach where possible. Management will follow appropriate procedures outlined within this document
Complaint from either a client, organisation or legal representative	Where there is a risk of complaint arising from the processing of data that may become a legal matter, processing must immediately cease. Strategic Management must be advised, and comprehensive guidance sought from the Information Commissioner's Office.	Immediately report to the Data Protection Officer and a strategic leader of the organisation. Management will follow appropriate procedures outlined within this document

The Information Commissioner's Office shall be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals, such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where there is a high risk to the rights and freedoms of individuals, they shall be notified directly.

Investigating Data Breaches

SPARCollective takes all data breaches seriously and will investigate all potential and actual data security breaches. The process for actual data breaches is noted below:

Containment and recovery – the following must be done within 72 hours of a breach:

- DPO shall identify the appropriate specialist, either internal or external, to investigate the breach and ensure they have appropriate resources

- The investigating party shall establish who needs to be made aware of the breach and inform them of what they are expected to do in terms of the containment exercise. This could be isolating a piece of equipment, finding a lost piece of hardware or changing the access codes to certain information
- The investigating party shall also establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause, as well as the physical recovery of equipment. Where appropriate, the police should be informed.

Assessing the risk – before deciding on steps beyond immediate containment

- What type of data is involved?
- How sensitive is the data?
- If the data has been lost or stolen, are there protections in place such as encryption?
- What has happened to the data and could it be used in a way that would be harmful to individuals?
- What could the data tell a third party about the individual(s)?
- How many individuals' data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there wider considerations such as a loss of public confidence?
- If bank details have been lost, consider contacting the banks for advice

Notification of Breaches – informing people when appropriate

- The DPO shall identify if there are any legal or contractual requirements to comply with in the event of a breach
- The DPO shall decide whether to notify the affected individuals by considering the risk to them and the part they can play in mitigating risk. Over notification should also be considered as a consequence of a breach
- If notifying individuals, they should be given specific and clear advice on the steps they can take to protect themselves, and also what SPARCollective is willing to do to help them
- The DPO shall determine if the Information Commissioner's Office needs to be notified
- The DPO should also determine which third parties require to be notified, such as the police, insurers, professional bodies.

It is important, not only to investigate breaches and their causes, but to evaluate the effectiveness of the organisation's response to it and the measures put in place to prevent recurrence. The DPO shall update documents, systems and procedures in response to incidents.

Disposing of Data

SPARCollective is committed to keeping personal data for the minimum time necessary to fulfil its purpose.

- Contact Data – will be disposed of six months after the contact is made (unless permission is sought to keep the data for longer)
- Employee Data - will be disposed of 5 years after the end of the individual's employment with the organisation, in order to meet needs for pensions, tax, potential disputes and references
- Health & Safety Data – SPARCollective will keep health & safety records of accidents that happen within the organisation for 3 years after the date of the accident.

Paper based products will be disposed of in a confidential waste sack or will be shredded. Electronic records will be deleted through either the decommissioning of equipment or the deletion of records from databases at source.

Requests for and Individual's Own Data

The rights of the Individual

Under Data Protection Legislation, an individual has the right to request all the personal data that an organisation holds about them. They also have the right to know the source of the data, and the purpose that it is being held for. The individual needs to make the request in writing by post.

If a verbal request is made, the individual should be informed that they need to put their request in writing. They should be provided with all necessary details to enable them to do this.

Individuals requesting access must provide some form of identification, and information about the data they are seeking. Subject to the verification of the individual's identity and the specific requirements, within one month of receiving the request, SPARCollective shall provide:

- Confirmation that their data is processed
- Access to their personal data
- Other supplementary information as outlined by law

Data we need to provide can include:

- Records of any contact with SPARCollective
- Information for payroll and other related purposes
- Research activity
- Records of any third parties that data has been shared with

Dealing with the Request

Preparations should be made (but not started) to gather all relevant documents relating to the request. It is important to provide all relevant documents to the Data Protection Officer, even if they are contentious.

The DPO will review each piece of documentation before it is released to the individual and will either redact, withhold or provide the data as part of the response to the request. The DPO will flag any documents which are contentious or sensitive.

An explanation will be given as to why there is concern over the release of such documents. This will help inform the response to the request but does not mean that the information will be able to be withheld. Information can only be withheld in very limited circumstances.