ROSCOMMON SPCA

Data Protection Policy

This Policy was approved & authorised by:

Name: Rose Harvey

Position: Chairperson

Date: 01/07/2018

Table of Contents

Executive Summary

Roscommon SPCA is a data controller of personal data relating to management, its past, present and prospective employees, volunteers, supporters, member of the public who contact us and various other individuals.

The introduction of the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), significantly increases the obligations and responsibilities on organisations such as Roscommon SPCA in relation to how it collects, uses and protects personal data. Roscommon SPCA recognises that the protection of peoples' personal data through appropriate processes, controls, and security is essential.

Everyone who works for, or with, Roscommon SPCA has a responsibility for ensuring personal data is processed correctly. The Committee of Roscommon SPCA have ultimate responsibility and have been tasked with ensuring best practice based on current practice is adhered to.

Roscommon SPCA has devised this policy which aims to provide pragmatic guidance for all staff and volunteers. All staff and volunteers are expected to become familiar with, and implement, the advice relevant to their specific role. Staff and volunteers should also apply good judgement to situations where they handle personal data. Further in-depth advice can be provided by management if complex situations arise.

Under the GDPR, data controllers must be able to demonstrate compliance and show transparency and accountability in respect of all core principles and requirements of the Regulation. To achieve this, Roscommon SPCA will follow the following core approaches:

- Privacy by design
- Privacy by default
- Risk mitigation

We will also:

- Document our core processing activities so staff, volunteers, and any contractors we engage, know the correct protocols and procedures to follow with respect to the handling of people's data.
- Conduct privacy impact assessments on any new technology or methods of working that could pose a high risk to the rights and freedoms of individuals.
- Ensure contracts are in place with third parties that provide appropriate controls and mitigations for data privacy issues and risks, as required under GDPR. We will highlight any remaining risks to the individuals concerned.

Roscommon SPCA is committed to ensuring the consistent delivery of privacy-respecting outcomes for staff, volunteers, clients and others and we strive to continuously improve our approach to data protection.

Introduction

This policy document aims to illustrate how Roscommon SPCA complying with its obligations under EU data protection law; that the organisation is open and transparent about the processing of personal data concerning living individuals; how it communicates and informs each person that they have rights in relation to how Roscommon SPCA use their personal data.

Our Committee:

Steven Hunter
Bridget Banham
Edward Conneely
Marie Farrell
Bernadette Murphy
Paul O'Sullivan
Una Davy
Breda McDermott
Rosie Carroll
Linda Kelly

Our Chairperson is: Rose Harvey.

All personal data collected and held by the Roscommon SPCA is protected by GDPR, in addition to the relevant legislation that transposes this into Irish law, the Irish Data Protection Act, 2018.

As a data controller and processor, we are fully cognisant of our responsibilities. We must gather, use and store certain information about individuals in order to provide our continuing service, that is the prevention of cruelty to animals, promoting animal welfare and to proactively relieve animal suffering in Ireland.

Data Protection Law

The GDPR is underpinned by seven core principles:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
Integrity and Confidentiality	Personal data shall 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
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

Vision Statement - Data Privacy at 1st July 2018

Our objective is to comply fully with the applicable Data Protection Law – which means:

(i) The Irish Data Protection Act 2018

(ii) The General Data Protection Regulation (Regulation (EU) 2016/679 (the "GDPR") and the successor to the ePrivacy Directive);

(iii) The European Communities (Electronic Communications Networks & Services) (Privacy & Electronic Communications) Regulations 2011;

(iv) The EU ePrivacy Directive 2002/58/EC (S.I. 336/2011) (as amended);

(v) All other industry guidelines (whether statutory or non-statutory) or applicable codes of practice and guidance notes issued from time to time by the Irish Data Protection Commissioner relating to the processing of personal data or privacy

It is within this context that Roscommon SPCA wishes to strive for compliance with the EU General Data Protection Regulation (GDPR) and recognise data protection as a human right under the EU Charter of Fundamental Freedoms.

Through our work we intend to actively promote high standards in the collection, processing, retention, and disposal of personal data. We will treat all personal information provided in a confidential manner and use this information only for the purposes for which it has been supplied, in accordance with the relevant legislation.

We will ensure that individuals can fully exercise their rights under the law and that our policies and procedures illustrate transparency and accountability, particularly in terms of data sharing with third parties.

In the event that we wish to collaborate with additional persons or organisations from the date of this policy, or wish to contract a new third-party vendor, we will assess each situation as it arises and apply best practice to the protection of personal information and the rights of individuals.

Roscommon SPCA pledges to make every effort to foster and embed an organisational culture that promotes data protection. We will strive to ensure that this vision statement for data privacy is known and understood by all our staff, volunteers, clients and other stakeholders.

Policy Scope

Everyone who works for, or with, Roscommon SPCA has some degree of responsibility for ensuring data is collected, stored and handled correctly. The Committee of Roscommon SPCA have ultimate personal responsibility for ensuring legal obligations are met and each manager should in turn ensure that best practice in data protection is adhered to in the department they have responsibility for.

This policy applies to the keeping and processing of Personal Data, in both manual and electronic form. Personal Data can include, but is not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photographs
- CCTV footage
- CVs
- Disciplinary records
- Any other information that identifies, or could potentially identify, an individual
- Physical and/or mental health information of members of the public (special category data)

Summary Policy Statement

Roscommon SPCA follows the following core approaches in relation to data privacy:

Privacy by Design

Prior to the introduction of any new system or methodology that utilises personal data, the protection of this data will be given careful consideration. We aim for this to occur as early as possible in the design process. We will consider the types and quantities of data collected, data flows and disclosures, data minimisation technologies and aim to show that adequate security is in place, whether for paper-based or digital records.

Where necessary, a formal Data Protection Impact Assessment (DPIA) will be undertaken, but in all cases, we will document the areas of risk and identify how we can ensure donors, persons and employee data is managed in the most privacy-respecting and security-supporting way possible.

Privacy by Default

In the roll out of any new system, process, or way of working at Roscommon SPCA, we ensure the highest standard privacy settings are automatically applied to the personal data of our internal and external customers. This approach is particularly salient in relation to the personal data of children.

We do not want our customers to have to think about how their privacy is being respected but instead we want them to trust that we are giving them appropriate choices and providing appropriate controls.

There is also a time sensitivity, as personal information must by default only be kept for the amount of time necessary to provide the product or service. We will continue to carefully monitor appropriate retention periods, followed by appropriate disposal, for each category of personal data that we hold. We will ensure that customers are fully aware why we collect their personal data and how long we hold it.

Risk based approach to data privacy

Roscommon SPCA consistently works to identify potential risks in the processing of personal data to enable us to swiftly address issues as they arise. The nature, context, scope and purposes of the processing is taken into account and balanced against the likelihood and severity of any risks posed to the rights and freedoms of individuals.

Roscommon SPCA strives to put in place technical and organisational measures that mitigate the risks to individuals' personal data through ensuring appropriate levels of security. These measures may include locked filing cabinets for paper records; pseudonymisation, anonymisation and encryption for digital files; as well as an ability to restore access to data in the event of a security incident. Regular testing, assessing, demonstrating and evaluating the effectiveness of these measures is also in place.

Roscommon SPCA is mindful of the requirements to notify the supervisory authority in Ireland (The Office of the Data Protection Commission, ODPC) of any potentially high-risk processing or relevant breach of personal data.

The Ethos of Accountability

Roscommon SPCA is aware that under the GDPR, data controllers and processors must be able to demonstrate compliance and show accountability in respect of all core principles and requirements of the Regulation.

We have put in place a range of processes that demonstrate efforts to achieve compliance. These processes vary depending on the complexity of the processing at hand and include the following:

- Assessing current practice and developing suitable data privacy governance structures
- Providing mentoring for staff and volunteers and to act as an initial point of contact for data subjects
- Creating a personal data inventory and ongoing audit practices
- Implementing appropriate privacy notices
- Obtaining appropriate consents from individuals where required for processing or retention of data
- Communicating the legal basis under which processes personal data
- Using appropriate organisational and technical measures to ensure compliance with the data protection principles
- Conducting regular risk assessments to ensure the fundamental rights and freedoms of data subjects are being upheld
- Creating an internal and an external breach reporting mechanism
- Actively monitoring the effectiveness of data protection policies and procedures and making amendments as deemed necessary

All staff and volunteers must be accountable for their own actions in relation to the processing of personal data. Staff and volunteers will be required to familiarise themselves with the personal data under their immediate control and ensure they take appropriate and logical measures to ensure it is handled with privacy and security in mind.

Regular staff and volunteer training and awareness events will be conducted as part of ongoing monitoring and evaluating of the effectiveness of policies and procedures. Every effort will be made to ensure adequate resources are allocated to provide the training and learning materials required to encourage compliance with data protection law.

All staff members or volunteers must comply with data protection procedures.

Data Privacy & Governance

Roscommon SPCA is committed to ensuring that personal data that has been collected and is processed with integrity and stored securely.

Roscommon SPCA operates from: PO BOX 10, Castlerea, Co. Roscommon

At any one time Roscommon SPCA can comprise of approximately 75 volunteers across the organisation.
Any person may contact us with regard to any aspect of the processing of their own personal data and to exercise their rights under the GDPR. These rights include:

- Right of access
- Right to rectification
- Right to be forgotten / erasure
- Right to restrict processing
- Right to be informed when their data is rectified, erased or restricted
- Right to object
- Right not to be subject to automated decision making and/or profiling
- Right to portability

Individuals must be allowed to exercise their rights free of charge unless the request is relatively onerous or the request is repetitive. Roscommon SPCA will also endeavour to ensure that requests from individuals will be responded to without undue delay, and within one month (although this timespan may be extended depending on the complexity involved and the number of requests received at any one time).

Procurement and Engagement of 3rd parties

Distinct obligations on data controllers are outlined in the Regulation which must be adhered to. Data processors must also fulfil certain obligations in tandem with offering full co-operation to data controllers to ensure compliant policies and procedures are in place.

As a data controller and as a data processor, Roscommon SPCA must conduct due diligence, have appropriate contract terms and change controls over contracts in place and must monitor and audit the services provided by third parties to ensure we are processing data in accordance with the Regulation.

We will ensure that we, and any third parties with who we share personal data with have appropriate security measures in place to ensure personal data is kept secure and confidential.

Third parties are also contractually obliged to assist Roscommon SPCA with notifying a supervisory authority or data subjects of any relevant data breach and assisting management in the carrying out of a DPIA.

All contracts with third parties are evidenced in writing. Any amendment to a contract with a third party relating to the obtaining, processing, storage, distribution, or destruction of data must be evidenced in writing and must be approved by general management. A copy of any amended instructions are appended to the master contract.

We ensure all contracted data processors are required to either delete or return all personal data to the organisation after the conclusion of processing activity.

Data Security Breach Notification Policy

Roscommon SPCA has endeavoured to put in place robust breach management and response policies. These include measures to help detect, react to and address a breach, as well as external notifications and subsequent communications across the organisation.

The GDPR introduces a duty on all data controllers and processors to report certain data breaches to the relevant supervisory authority, and in some cases to the individuals affected.

It is important for all staff and volunteers to be cognisant of the fact that a breach is more than just losing personal data. A personal data breach can also mean a breach of security leading to the destruction, alteration, unauthorised disclosure of, or access to, personal data.

It is vital that everyone who works for, or with, Roscommon SPCA (including volunteers) takes responsibility, in their role, for preventing breaches of personal data.

General guidelines:

- Staff and volunteers should only access data they require for their work.
- Data should not be shared informally under any circumstances.

- Staff and volunteers should keep all personal data secure, by illustrating good judgment and taking sensible precautions.
- Staff and volunteers should never leave paper files containing personal data unattended in any location where they can be accessed in an unauthorised fashion.
- All portable digital equipment or devices must be encrypted and kept on the person at all times.
- The forwarding of sensitive information by email, or over the internet, should only be done in a secure, encrypted manner.
- Staff and volunteers should be cautious that information is not inadvertently forwarded outside of Roscommon SPCA by email, SMS, MMS, via social media, fax or post.
- Any personal data stored in filing cabinets or rooms should be locked when not in use.
- Strong computer passwords or pin codes must be used and they should never be shared.
- Personal data should never be disclosed to unauthorised individuals.
- Personal data should be regularly reviewed and updated if it is found to be out of date.
- Personal data that is no longer required should be deleted, destroyed or in any manner, disposed of.
- Failure to comply with this policy may result in disciplinary action.

If a breach or suspected breach occurs, which could pose a risk to individuals, the manager or staff member/volunteer concerned should report it to Bridget Banham on 087 050 5594 immediately (including weekends) who will decide if the incident is sufficiently serious to notify the client and/or the ODPC.

If you discover a personal data security breach, please notify Bridget Banham by telephone immediately. Then please complete the form below and return it to Bridget Banham. This form is part of our regulatory reporting requirement to ensure correct reporting.

All sections must be completed in full. It's your responsibility to find the required information. The form is the only source of information for the Bridget Banham for reporting this matter to the ODPC so all available relevant information needs to be included.

Date(s) of Breach:	
Date Incident was discovered:	
Name of Person Reporting Incident:	
Contact Details of Person Reporting Incident:	
Brief Description of Personal Data Security Breach:	
Number of Data Subjects affected – if known:	
Brief Description of any action since breach was discovered:	

Roscommon SPCA reaction plan to any breach of personal data includes the following advice:

- Gather an immediate detailed description of the nature of the personal data likely to have been contained in the breached documents or digital files.
- Ascertain the categories and approximate number of individuals affected.
- Describe the likely consequences or risks that may flow from the personal data breach.
- Ascertain the recipient or likely recipient of the personal data.
- Consider the engagement of outside data protection advisors to perform an analysis and possible technical forensic assessment of the breach.
- Identify the measures that can be employed to mitigate any risks caused by the breach, such as isolating the cause and/or replicating any affected data.
- Consider whether external notification action is required. If deemed necessary, the ODPC will be contacted without delay and within 72 hours of becoming aware of the breach. Where the notification to the ODPC is not made within 72 hours, it shall be accompanied by reasons for the delay. If deemed necessary individuals affected will be contacted without undue delay.

- Consider whether an internal communications plan should be executed across the organisation to better educate and inform staff and volunteers.

If a suspected, or actual, breach of personal data takes place management, staff and volunteers are expected to act in accordance with the organisation's breach protocol.

If you suspect that the personal data of a member of the public, a donor or a volunteer has been

- lost;
- damaged;
- erased without consent;
- sent to other people or organisations without their consent or
- subject to hacking/malware/ransomware, you must contact Bridget Banham immediately on 087 050 5594 and onspca@roscommonspca.ie the data breach form above.

Conclusion

The new GDPR means we must take a proactive approach to data privacy by creating a data privacy standard and privacy control framework, which is then applied consistently across all functions and locations, minimising complexity and maximising data protection.

Such a framework has been followed by creating a data privacy strategy that helps us correctly manage the life cycle of personal data from collection, storage to disposal.

At Roscommon SPCA we are committed to ensuring the robust delivery of privacy-respecting outcomes for all staff, volunteers, donors, supporters and members of the public. This goal drives our wish to continuously improve our approach to data protection and we welcome feedback.

Appendix 1 - Core Definitions of the GDPR

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes

and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

'personal data' means any information relating to an identified or identifiable individual (**'data subject'**); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Appendix 2 - Description of Core Data Processing Activities

Volunteer applications form and personal details are stored securely.
Mailing list is secured securely on a computer.

Appendix 3 – Retention Policy

Once a volunteer is no longer involved with us, their personal information is deleted from our records.

Complaint forms are kept for 3 years.

No signing in books.