# Data Protection Policy

**Table of Contents**

**Section 1 - Introduction**

**Section 2 - Definitions**

**Section 3 - Data protection principles**

**Section 4 - Features of GDPR for special attention**

**Section 5 - Roles and Responsibilities**

**Section 6 - Advice/Assistance**

**Appendices:**

**Appendix 1 ACDI Subject Access request form**

**Appendix 2 – ACDI Ireland Data Breach Incident Notification Form**

**Section 1 – Introduction:**

Aoife’s Clown doctors are experienced performers who transport vulnerable and sick children in hospital to a world of wonder and fun. Their interactive clowning around allow the children and their families to laugh, experience joy and have a brief escape from what can be a frightening reality.

ACDI operates in line with General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

The aim of this policy is to outline the concepts of Data Protection and ACDI’s responsibilities in relation to the organisation’s overall compliance with GDPR.

This policy will outline these concepts in relation to the following categories:

1. Consent for promotion on Social media/promotional material: From parents/guardians regarding use of childrens’ photos and names (personal data)
2. Consent: Collecting basic donor contact details/photos for receiving and acknowledging donations (personal data)
3. Contract: Relating to payment and scheduling of self employed Clown Doctors

**Section 2 – Definitions:**

**Data Protection** is the safeguarding of the rights of individuals to privacy and integrity in relation to the processing of their personal data.

**Data Controller (Ashling Fitzpatrick)** is the natural or legal person (most charities or non-government organisations are data controllers) who, alone or jointly with others, determines the purpose and means of the processing of personal data. In other words, the controller decides what personal data will be processed for and how it will be done.

**Data Processor** is the legal person such as an individual or a company who processes personal data on behalf of a controller

**Data Subject** is an individual who is the subject of personal data.

In ACDI **the Data Protection lead (Ashling Fitzpatrick)**is the individual within an organisation who has responsibility for data protection.

**Data** means information in any form, which can be processed. Types of data incl.:

* **Personal data** is any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person 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 natural person.
* **Special categories of personal data** (this term replaces the term *sensitive personal data*) is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.
* **Genetic data** is personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
* **Biometric data** is personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.
* **Automated data** means any information created and held on computers, e.g. a word document, an email or a database.
* **Manual data** means information that is kept as part of a relevant filing system or with the intention that it should form part of a relevant filing system, e.g. traditional paper files, personnel and financial records which are used as part of our daily operational duties.

**Relevant filing systems** means any sets of information, which are not computerised but are structured by reference to individuals or by reference to criteria relating to individuals so that specific information relating to a particular individual is readily accessible.

**Pseudonymisation** is 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 is not attributed to an identified or identifiable natural person.

**Subject access request** – people have a right to request a copy of data we hold on them from the data controller. Under GDPR this needs to be provided free and within 1 month (30 days). It is essential that such a request is recognised as urgent as passed onto the relevant staff person as quickly as possible.

**Data 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.

**Section 3 - Data Protection Principles:**

The 7 data protection *principles* are the fundamental principles relating to how personal data may be processed. ACDI must adhere to these principles at all times:

1. Lawful, fair and transparent processing:
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability
8. **Lawful, fair and transparent processing:**

ACDI will process personal data based on one or more Lawful Processing Conditions ie:

* Consent: the Data Subject has clearly and willingly agreed to the processing of their personal data for one or several purposes. An unambiguous indication of the data subject’s wishes by a statement or clear affirmative action is needed.
  + Consent for promotion on Social media/promotional material: From parents/guardians regarding use of childrens’ photos and names
  + Consent: Collecting basic donor contact details/photos for receiving and acknowledging donations. Donors contact ACDI to inform them that they are fundraising or donating to ACDI. Only contact details are given. ACDI forward them the bank details for transfer of funds. Their name is recorded on a spreadsheet alongside the sponsored clown round and they are acknowledged on social media. See log for more details
* Contract: the processing activity is necessary for the performance of a contract between the Controller and the Data Subject, or necessary at the request of the Data Subject prior to entering into a contract.
  + Contract relating to payment and scheduling of self-employed Clown Doctors. The clown doctors invoice ACDI and they are paid through direct debit. Basic contact details are stored for communication re: scheduling.
* Legal Obligation: the processing is necessary for compliance with a legal obligation to which the Controller is subject.
* Vital Interests: the processing of the personal data is necessary in order to protect the vital interests of the Data Subject.
* Public Interest / Official Authority: the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official, regulatory or statutory authority, which is vested in the Controller
* Legitimate Interest: the processing is necessary for the purposes of the legitimate interests pursued by the Controller or the Processor, except where these are overridden by the interests or fundamental rights and freedoms of the Data Subject, particularly where he or she is a child.

See ACDI processing log for more details

1. **Specified and Lawful Purpose:**

ACDI will process personal data on the basis of one or more specified purposes i.e. data collected for 1 reason and cannot be used for a different reason

* + ACDI does not use photos/videos for any other purpose than that for which consent was given. Personal data/contact details are not used for any other purpose than agreed e.g. Donors are not contacted for other fundraising campaigns.

1. **Minimisation of processing:**

ACDI will collect personal data limited to what is necessary. ACDI can fulfill this requirement by making sure they only seek and retain the minimum amount of personal data needed for the specified purpose. It should be retained for no longer than is necessary for the purpose or purposes.

* + Only photos and names are requested for promotional/acknowledgement purposes.
  + Only relevant basic donor information is requested.
  + Self-employed Invoices will only be kept as long as is necessary for accounting purposes.

See ACDI processing log for more details

1. **Accuracy:**

ACDI will ensure personal data collected is accurate, and where necessary, kept up-to-date. A data subject is entitled to have inaccurate personal data concerning themselves rectified without delay, incomplete data concerning themselves completed and to have personal data about them erased. The right to erasure relates to situations where the data subject withdraws consent, objects to the processing or where the personal data has been unlawfully processed, among other reasons. However, the right to erasure is not available where the processing of the relevant personal data is necessary for the establishment, exercise or defence of legal claims, among other reasons.

* + Clown doctor invoices are sent regularly so this ensures that all data is always up to date. Photos/Names/Posts will be removed at DS request.

1. **Storage limitation:**

ACDI will keep personal data for no longer than is necessary. Exceptions can be made where a donor or other legitimate regulation sets the criteria for retention period. This requirement places a responsibility on ACDI to be clear about the length of time data will be kept and the reason why the information is being retained. To meet this requirement, ACDI will ensure that all files are managed and appropriate retention/disposition schedules are in place. See ACDI processing log for more details

1. **Security and confidentiality:**

ACDI will process personal data 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.

The minimum standard of security that is expected includes:

* computer systems password protected and passwords must not be disclosed
* access to information restricted to authorised staff on a ‘need to know’ basis
* Paper files/invoices stored in locked cabinet.

GDPR places serious responsibility on every employee not to disclose data in relation to any individual to any other individual who is not entitled by law to receive it. . Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which the data is collected and kept.

1. **Liability and accountability:**

ACDI will be able at all times to demonstrate how it complies with GDPR. One staff member with an overarching responsibility for Data Protection will retain an up-dated folder containing a copy of:

* ACDI’s Data Protection Policy
* ACDI Data Process Log Spreadsheet

**Section 4 – Matters for special attention**

**The GDPR introduces a number of specific requirements relating to the processing of children’s data:**

* Specific protections must be applied to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.
* ACDI receive consent from children’s parents/guardians to use images/videos/names online/promotional materials

**Data Subject Rights and Freedoms:**

Besides the 7 data protection principles above, the GDPR strengthens existing rights and freedoms of the Data Subject and introduces new rights and freedoms.

* Right to be Forgotten: this right to erasure of personal data allows the Data Subject to request from the Controller the deletion of personal data, without undue delay, on particular grounds. ACDI will delete any photos when requested without delay
* Right to Restriction of Processing: in certain circumstances, the Data Subject can request ACDI to restrict processing either permanently or temporarily. For example, a Data Subject could ask ACDI not to publish a photograph from a fundraising event showing his or her face until the lawful processing condition for this is clarified.
* Right to Object to Certain Processing: the Data Subject is entitled to object to the processing of their personal data based on his or her situation, preference or state of mind. Where data is processed, for example, for the purpose of direct marketing, consent may be withdrawn at any time and free of charge.
* Right to Data Portability: where a Data Subject is moving their account from one provider to another (or one organisation to another), the Data Subject should be able to receive a copy of his or her personal data in a structured, commonly used, machine readable format.
* Right of Access to Information: the Data Subject has the right of access to their personal data which was collected concerning him or her and can exercise that right easily and free of charge. ACDI must respond within 30 days (one calendar month) of receiving the valid, written request. See Appendix 1 – ACDI Subject Access Request Form.Every Data Subject has the right to know, from ACDI:
* Who processed their personal data where, when and how;
* Why such data was processed;
* For how long such data was processed
* The recipients of the personal data
* Where applicable, the logic involved in automatic processing, including profiling and the consequences of such processing.

In addition, the requestor will be entitled to a copy of any personal information held by ACDI which relates to him or her.

* Right to Complain, Right to Judicial Remedy: where a Data Subject is not satisfied that ACDI adhered to its obligations under the GDPR, he or she can consider bringing a complaint to the Data Protection Commissioner or seek a judicial remedy in the Irish courts.

**Data Protection by Design and Default:**

The GDPR contains the new concepts of privacy by design and by default, intended to strengthen the protection of privacy by requiring organisations to build consideration of privacy into their product and service design processes in certain cases. Privacy by Design requires organisations to consider privacy measures during product design processes, while Privacy by Default requires controllers to ensure that, by default, only necessary data is processed. Privacy Impact Assessments (PIAs) must be carried out prior to any new development, system change or operational change to ensure these developments are in line with the ‘by design and default’ requirement. The Office of the Data Protection Commissioner provides clear guidance on PIA implementation.

**Data Breach:**

ACDI will take every care to avoid a data protection breach that could compromise security. ACDI is obliged under the GDPR to have in place procedures to ensure the security of all personal data during its lifecycle.

A data breach includes but is not restricted to:

* Loss or theft of personal data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device or paper record)
* Equipment theft or failure
* Unauthorised use of, access to or modification of data or information systems
* Attempts (failed or successful) to gain unauthorised access to information or IT systems
* Unauthorised disclosure of personal data
* Website defacement
* Hacking attack
* Unforeseen circumstance such as a fire or flood
* Human error
* ‘Blagging’ offences where information is obtained by deceiving the organisation that holds it

Any individual who accesses, uses or manages ACDI’s information is responsible for reporting data breach and information security incidents immediately to Ashling Fitzpatrick using the ACDI Data Breach Incident Notification Form (see Appendix 2). Appropriate steps will be taken immediately to minimise the effect of the breach, assess how/why it happened, take steps to mitigate such a breach being repeated and notify all relevant parties of the breach. Under the GDPR, breach notifications to the Data Protection Commissioner are mandatory within 72 hours of first noticing the breach ‘unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.’

**Data exchange relationships:**

The GDPR provides for two data exchange relationships:

Relationship 1 - The GDPR requires ACDI (as Data Controller) to enter into a Data Processing Agreement with each Data Processor who is involved in the processing of personal data on ACDI’s behalf. This contract needs to be in writing and must cover certain basic requirements, such as guarantees concerning the safety and security of data, auditing rights, cooperation concerning the rights and freedoms of Data Subjects.

Relationship 2 - Where organisations collaborate on a peer-to-peer basis to achieve a particular objective, both parties retain their Data Controller status. The GDPR designates this as a Joint Controller relationship, and requires that a Data Sharing Agreement is in place, rather than a Data Processor Agreement.

**Processing Logs:**

All data processing activities need to be logged in a transparent and auditable manner in a Process Log Questionnaire

**Section 5 - Roles and Responsibilities**

**ACDI overall data protection lead:**

ACDI’s overall data protection lead is Ashling Fitzpatrick

**Board Members:**

ACDI board members are responsible for ensuring that all data that they access, manage and control as part of their duties is done in accordance with this policy and must also ensure their personal information provided to ACDI is accurate and up-to-date (e.g. informing ACDI of change of address or other circumstances).

**Data Protection Commissioner:**

The Commissioner is appointed by Government and is independent in the exercise of his or her functions. Individuals who feel their rights are being infringed can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it. The commissioner’s office is a good source of guidance on all data protection matters. See [www.dataprotection.ie](http://www.dataprotection.ie)

**Section 6 - Advice/Assistance**

For in-house advice or assistance please contact:

* Ashling Fitzpatrick (ACDI overall data protection lead), email: info@aoifesclowndoctors.ie Address: Aoife’s Clown Doctors Ireland, 1A New Street Skerries Dublin K34T864

Externally, the Data Protection Commissioner’s office is contactable at [info@dataprotection.ie](mailto:info@dataprotection.ie) / Lo Call no.1890 252 231 / [www.dataprotection.ie](http://www.dataprotection.ie) / [www.GDPRandYOU.ie](http://www.gdprandyou.ie)

**Appendix 1 – Aoife’s Clown Doctors Ireland Subject Access Request Form**

1. Name & Address
2. Tel. No.
3. Email
4. What is your link to ACDI? Please give details

1. Is the information about you? If yes, you will need to provide a copy of photographic ID, bearing your signature, for example, a passport or driving licence.
2. Please describe what information you require with any additional facts that may help us with the search.
3. **Declaration to be completed by all applicants.**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (name), certify that the information given on this application to ACDI is correct. I understand that it is necessary for ACDI to confirm my identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Note**: ACDI must respond to your request within one calendar month/30 days. This time frame will not begin until your identity has been established and any relevant details obtained.

Please return the completed form and any necessary documentation to Aine Hendrick**,** Aoife’s Clown Doctors Ireland, 1A New Street Skerries Dublin K34T864

Documents which must accompany this application include evidence of identity; and stamped address envelope for return of the above mentioned documents.

*ACDI will process the personal information included on this form in accordance with GDPR.*

**Appendix 2 –Aoife’s Clown Doctors Ireland Data Breach Incident Notification Form**

**Data Breach Incident Notification Form**

The purpose of this document is to report a Breach Incident involving Personal Data, as required under General Data Protection Regulation from 25 May 2018. ACDI is committed to protecting the confidentiality and integrity of the personal information under its control, and will ensure that such incidents are appropriately investigated and reported, and that the risk of a recurrence is minimised.

**Contact Information**

|  |  |
| --- | --- |
| **Data Controller/Organisation:** |  |
| **ACDI overall data protection lead:** |  |
| **Contact details:** |  |

**High Level Description of Incident**

|  |  |  |
| --- | --- | --- |
| **Brief Description of Incident:** |  | |
| **Date of Incident:** |  | |
| **Location of Incident (if known):** |  | |
| **Date and time when Controller was made aware (if different):** | **Date:** | **Time:** |

**Personal Data Impacted by Incident**

|  |  |
| --- | --- |
| **Description of Personal Data / Sensitive Personal Data impacted:** |  |
| **Categories of Data Subjects impacted:** |  |
| **Volume of records involved:** |  |
| **Number of Data Subjects impacted:** |  |

**Detailed Description of the Incident**

|  |
| --- |
| *(Description of the sequence of events leading up to the breach incident - please include associated e-mail correspondence)* |

**Actions taken (to date) to address the Incident**

|  |
| --- |
| *(Description of the measures which have been taken since becoming aware of the Incident)* |

**Current Status (At time of reporting)**

|  |
| --- |
| *(What is the current status of the Personal Data impacted by the breach incident?)* |

**Actions being taken to minimise impact on Data Subjects**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Description** | **Owner** | **Status (planned, under way, complete)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Actions being taken to prevent a recurrence of the incident**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Description** | **Owner** | **Status (planned, under way, complete)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Reporting to External Agencies or Individuals**

*(Where information on the incident has been communicated to an external party, either corporate or individual, please attach a copy of the communication)*

|  |  |
| --- | --- |
| **External agency 1** |  |
| **Details of Reporting Obligation (Regulatory, Legal, Data Subject, Insurance)** |  |
| **Date of Incident Notification** |  |
|  |  |
| **External agency 2** |  |
| **Details of Reporting Obligation (Regulatory, Legal, Civil, Insurance)** |  |
| **Date of Incident Notification** |  |
|  |  |
| **External agency 3** |  |
| **Details of Reporting Obligation (Regulatory, Legal, Civil, Insurance)** |  |
| **Date of Incident Notification** |  |