

Data Protection Policy

May 2022

# Policy Statement

Eventi Management is committed to ensuring Data Protection in all forms throughout all our projects.

Personal Privacy Rights

Anyone who Eventi Management works with is entitled to the following rights:

* Have access to what information we hold on you
* Have inaccuracies of your information corrected
* Have all your information erased
* Object to direct marketing
* To restrict the processing of your information, including automated decision-making
* Data portability

Access to Information

Access to information can be requested from Eventi Management using the contact details supplied at the bottom of this page.

Data Retention

Eventi Management will hold all documents in line with the table provided in this document.

A request can be submitted to delete and remove part, or all your information held by Eventi Management. However, we will require proof of identification.

Signed release documents that are required for legal purposes will be held at the discretion and advice of the Data Protection Commissioner.

Data Protection Impact Assessment (DPIA)

Eventi Management will perform a Data Protection Impact Assessment as necessary, in line with the General Data Protection Regulation. DPIA’s will be held on file and can be requested from the Eventi Management office.

Contact Details

You can contact Eventi Managementthrough the following methods:

Telephone: *+353 (0)21 4553095*

E-mail: *info@eventi.ie*

Post: *Eventi Management, 12 Mulgrave Road, Shandon, Cork.*

## Purpose of Policy

This policy is written to describe Eventi Management’s policy and procedures in respect of data protection

To provide details of how Eventi Management manages personal and corporate data, and how this data is processed in line with statutory obligations.

## Definitions

* Data – Information in a form that can be processed (including both automated and manual data)
* Processing – Performing any operation or set of operations on data including:
* Obtaining, recording, or keeping data
Collecting, organising, storing, altering, or adapting data o Retrieving, consulting, or using data
* Disclosing the information or data by transmitting, disseminating, or otherwise making it available
* Aligning, combining, blocking, erasing, or destroying data
* Personal Data – Data relating to an individual who can be identified by the data or in conjunction with other information (that is likely in possession of the data controller)
* Sensitive Personal Data – Relates to specific categories of data which are defined as data relating to a person’s racial origin; political opinions; religious/or other beliefs; physical and/or mental health; criminal convictions or alleged commission of an offence; trade union membership;
* Data Subject – An individual who is the subject of personal data
* Data Controller – Those who, either alone or with others, control the contents and use of personal data. (i.e. ARTlifeCULTURE)
* Individual/Client/Young Person/Parent – is an individual who uses the services of ARTlifeCULTURE and on whom ARTlifeCULTURE keeps personal data
* Staff Member – An individual who works with ARTlifeCULTURE and on whom ARTlifeCULTURE keeps personal data. This includes both employees, volunteers, students, and locums
* GDPR – General Data Protection Regulation

## Personal Privacy Rights

Anyone who Eventi Manahement works with is entitled to the following rights:

* Have access to what information we hold on you
* Have inaccuracies of your information corrected
* Have all your information erased
* Object to direct marketing
* To restrict the processing of your information, including automated decision-making
* Data portability

## Roles and Responsibilities

The members of the Designated Liaison Panel (including the Data Protection Officer) are responsible for data protection issues in the company. The panel is responsible for:

* Addressing all queries in relation to data protection • Ensuring that this policy is kept up to date
* Overall implementation of this policy
* Ensuring staff are familiar with this policy

Staff members hold the responsibility of:

* Being familiar with the policy
* Ensuring the procedures in data management and protection are followed (if specific to role)
* Reporting data protection concerns to the Designated Liaison Panel or Data Protection Officer
* Staff members who deal with personal information should take extra care with this information

Record keeping, and data protection procedures and responsibilities will form a part of the induction process for staff.

## Storing Data

### Manual Data

Any manual data will be kept by Eventi Management in a manner consistent with good data retention.

* All personal data will be kept in a private office with access to Eventi Management employees only
* When transporting private data, this will be kept in a secure case or folder, so that data is only available to relevant Eventi Management staff
* All records should be written legibly and indelibly. Records should be clear, unambiguous, and accurate, including date and the printed name and signature of the person completing the record
* Alterations are made by scoring out with a single line followed by the initialled and dated correct entry (the use of correction fluid such as ‘Tipp-Ex’ is not permitted)
* Records are not to include jargon, subjective statements, or abbreviations other than those in common organisational use. All records should be written in a way that is easy to understand
* Records should include only essential and relevant details

### Automated Data

The principals for manual data also apply to automated data. In addition:

* Staff must ensure that computerised records are not left unattended (e.g. lock computerised systems)
* All computerised systems that hold personal data must be password protected, and these must be changed regularly
* In accordance with good data retention passwords should not be written down
* Data on computerised systems should be backed up regularly on an appropriate data storage back system.

## Data Retention

### Retention Precautions

* Precautions should be taken to protect written copies from damages due to fire, and water
* Precautions should be taken to protect all electronic data from viruses or technical failure
* Systems should be secured to protect against hacking attempts (within reasonable limits)
* Data management systems should be monitored regularly
* Data management should be reviewed every year to ensure that data isn’t kept for longer than it needs to be.
* In the event of unspecified data, a blanket period of six years will apply in respect of retention
* Data related to Incident Reports, Child Protection Concerns, ongoing legal and investigative actions should not be destroyed
* Data needs to be destroyed or disposed of correctly and securely. Any paper material containing personal details need to be shredded to ensure data protection.

### Retention Periods

|  |  |
| --- | --- |
| **Type of Data** | **Retention Period** |
| Participant Records | 6 years after cessation of participation in any project |
| Consent Forms | 6 years after project |
| Group Records | 3 years |
| Necessary Medical Records | 6 years after cessation of employment or volunteering |
| Meeting Records (Including DLP meetings) | 3 years |
| Recruitment Records | 6 years after cessation of employment or volunteering  |
| Application Forms and Interview Notes (unsuccessful candidates) | 1 year |
| Staff and Training Records (including disciplinary records and working time records) | 6 years after employment ceases |
| Staff Certificate Records |  |
| Proof of Identification/Age | Copies of documents to be destroyed once they have fulfilled their purpose |
| Interagency/Partnership Records | 6 years |
| Tax Records | Not less than 5 years after the financial year to which they relate |
| Accounting Records | 6 years |
| Maternity, Sick Leave, Holidays, Public Holidays, and Rest Period Records | 3 years after the end of the tax year in which the holiday period ends |
| Salary Records (including overtime, bonuses, expenses) | 6 years |
| Programme Records | 3 years |

## Access Controls

### Access to Information by Staff Members

Any access to data containing personal information is strictly limited to a “need to know” basis. However, for an effective integrated response to the needs of service users, all staff members involved in supporting an individual will “need to know” relevant personal information.

### Sharing Information with External Agencies or Organisations

Eventi Management might need to share limited personal data with external agencies or organisations (e.g. Sharing dietary requirements, or medical information in emergency cases). This will be requested from the parent/guardian/individual when signing the application/consent form.

### Sharing Information in Children and Vulnerable Persons Safeguarding Situations

In the case of reports made on the basis of Child Protection and/or Vulnerable Persons Safeguarding concerns it is our practice to notify the parents/guardians. This applies unless Eventi Management feels that this puts a Child and/or Vulnerable Person in immediate danger. In these cases, Eventi Management will share information with the necessary agencies/statutory bodies without the expressed permission of the individual/young person/parents/guardians in line with Eventi Management’s *Children and Vulnerable Person Safeguarding Policy.*

## Access for Data Subjects

Data subjects have the right to access the data that Eventi Managment holds on them. In order to access this information, they need to request this in writing to the following:

*Sinéad Dunphy, Eventi Management, 12 Mulgrave Road, Shandon, Cork.*

### Access Request Procedure

The Data Protection Officer or member of the Designated Liaison Panel will process the Access Request and will send an acknowledgement of receipt and a description of details held by Eventi Management within 21 days of receiving the request.

The following will happen within 40 days of the receiving the request:

* The Data Protection Officer/Designated Liaison Panel will ask the Data Subject why they require this information, and if they want a specific piece of information or all the data that we hold on the data subject. It is important to note that the Data Subject is not required to provide a reason as to why they want to data, and this does not affect theirright to receive their personal data
* An appointment will be made with the Data Subject to meet the Data Protection Officer who will then provide the data required. The data will only be given to the individual to which the data belongs or to someone acting on their behalf who has pre-arranged written authority
* Young people can request access to their data, only if Eventi Management are of the opinion that the young person has the sufficient intellectual ability to understand the nature of the request
* Parent/guardians have the right to request access to their children’s data in the case that their child does not have the intellectual ability to understand the nature of the request, and if the parents/guardian are acting in the best interest of the child. (A request will not be acceded if it would likely be relevant to any ongoing abuse/welfare allegation that may involve the requester
* A copy of the records will be collated. All information relating to other people will be excluded or erased from that copy. Particular care needs to be taken when suppling information/records that contain information relating to other people, and this should be erased using black permanent marker in the record copy
* Present the records to the person requesting the data (provided they have permission and have identified themselves) and offer to take them through the records. When necessary, explain how the different records are used and to answer and questions a person may have
* Explain that any information requested will be copied for the purpose of supplying the requestee with the data/records, but that all original data/records will be kept securely on file

## Complaints Procedure

In the event that a Data Subject is not happy with the management of personal data, they have the right to make a complaint about this to Eventi Management and the Data Protection Commissioner. Eventi Management will support any Data Subject in making a complaint to the Data Protection Officer should they request to do so.

### Complaint to Eventi Management

A complaint can be made directly to Eventi Management in writing which contains the following:

* + Name of Data Subject to which the data is relevant
	+ Name of complainant (if this isn’t the Data Subject)
	+ Why the complaint is made and if it relates to a specific piece of data or to a process
	+ Date on which the complaint is made
	+ Signature of complainant

This request needs to be sent to:

*Sinéad Dunphy, Eventi Management, 12 Mulgrave Road, Shandon, Cork.*

Any complaint will be processed within 40 days and an acknowledgment will be sent to the complainant.

### Complaint to the Office of the Data Protection Commissioner

Data subjects are encouraged to make a complaint to the Office of the Data Protection Commissioner should they feel the need to do so.

* Information on how to do so can be found using the following:
* Website: http://www.dataprotection.ie
* Telephone: 1890 252 231
Email: info@dataprotection.ie
* Address: Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, Ireland

## Key Legislative Provisions

This policy is written and is in accordance with the following guidelines and pieces of legislation:

* The Data Protection Act 1988
* The Data Protection (Amendment) Act 2003
* The Freedom of Information Act 1997
* The Freedom of Information (Amendment) Act 2003
* General Data Protection Regulation 2008
* Data Protection Bill 2018 (Prospective)