Data Protection Policy

Table of Contents

Overview

In order to carry out *Business to Arts* day-to-day activities, we need to collect and maintain information about our Corporate Patrons, Members, Arts Affiliates, entrants to the Allianz Business to Arts Awards, artists/arts organisations and stakeholders who are involved in our programmes, open calls and events run by the organisation at the *Business to Arts* office and other locations. This policy will be reviewed each year. Fundit.ie operated by *Business to Arts* has its own independent Data Protection Policy.

PART 1: Policy

1.1 GDPR Protection Principles & Accountability

Under the EU General Data Protection Regulation (GDPR) which came into force on 25th May 2018. *Business to Arts* has the legal responsibility to comply with the principles of data protection including:

- Data collection must be fair and for a legal purpose. We must be open and transparent as to how the data will be used.
- The data we collect must be for a specific purpose. Any data collected must be necessary and not excessive for its purpose.
- The data we hold must be accurate and kept up to date
- We cannot store data longer than necessary.
- The data we hold must be kept safe, secure and confidential

1.2 Policy Statement

Business to Arts aims to:

- Comply with the Data Protection Acts, GDPR Regulations and good practice
- Protect the privacy rights of the people we support and the staff of *Business to Arts* in accordance with Data Protection legislation
- Ensure that Personal Data in *Business to Arts'* possession is kept safe and secure
- Support staff to meet their legal responsibilities as set out in the Seven Data Protection Principles

1.3 Policy Purposes

The purposes of this Data Protection Policy are:

- To outline how *Business to Arts* aims to comply with GDPR
- To provide good practice guidelines for staff
- To protect *Business to Arts* from the consequences of a breach of its responsibilities

1.4 Policy Scope

This Policy applies to all staff who handle Personal Data of the people we support and/or staff.

1.5 Definitions/ Descriptions

'Access Request' is where a person makes a request to an organisation for the disclosure of their Personal Data, under section 4 of the Data Protection Acts.

'Data' is information in a form that can be processed. It includes automated or electronic Data (any information on computer or information recorded with the intention of putting it on computer) and manual Data (information that is recorded as part of a Relevant Filing System, or with the intention that it should form part of a Relevant Filing System).

'Data Controller' is a person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.

'Data Protection Officer' is a person who (either alone or with others) controls the contents and use of Personal Data. (*Business to Arts* as a 'legal person' is a Data Protection Officer).

'Data Processing' is the performance of any operation or set of operations on data, including:

- Obtaining, recording or keeping the Data
- Collecting, organising, storing, altering or adapting the Data
- Retrieving, consulting or using the Data
- Disclosing the Data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking, erasing or destroying the Data

'Data Processor' is a person who processes personal information (Data) on behalf of a Data Protection Officer, but does not include an employee of a Data Protection Officer who processes such Data in the course of his/her employment; for example, this might mean an employee of an organisation to which the Data Protection Officer out-sources work. The Data Protection Acts places responsibilities on such entities in relation to their processing of the Data.

'Data Subject' is an individual who is the subject of Personal Data.

'Personal Data' is Data relating to a living individual who is or can be identified, either from the Data or from the Data in conjunction with other information, which is in, or is likely to come into the possession of the Data Protection Officer. It includes information in the form of photographs, audio and video recordings, and text messages.

'Relevant Filing System' is any set of information organised by name, date of birth, PPSN, payroll number, employee number, or any other unique identifier.

'Sensitive Personal Data' relates to specific categories of Data which are defined as Data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions, or the alleged commission of an offence; trade union membership.

The Data Protection Acts 1988 & 2003 (the 'Data Protection Acts') confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling Personal Data.

PART 2: General Guidelines

2.1 Introduction

GDPR Regulations confer rights on individuals, as well as placing responsibilities on those persons processing Personal Data. *Business to Arts*, endeavours to meet its legal responsibilities in relation to the information it processes. This involves the obligation on all staff involved in processing Personal Data to apply the Seven Data Protection Principles, in order to safeguard the privacy rights of individuals.

Data will be kept for specified, explicit and lawful purposes, as set out below:

- For Corporate Patrons, Members & Friends: personal data will be collected and kept so that *Business to Arts* staff may contact Members about their membership or affiliate of *Business to Arts* and participation in membership programmes
- For Award entrants: Organisational data will be collected and kept so that *Business to Arts* for the purposes of contacting entrants about *Business to Arts* initiatives that may be relevant to them
- For Artists/Arts organisations: Data will be collected and kept for the purposes of engaging and participation in *Business to Arts* affiliate programmes
- For Staff and Board: Personal data will be kept and maintained as part of the employment contracts and Governance of organisation

2.2 Lawful, Fair and transparent processing of data

To **fairly, lawfully and transparently obtain information**, the Data Subject must, at the time their Personal Data is collected, be made aware of the following:

- The purpose in collecting the Data
- The persons or categories of persons to whom the Data may be disclosed
- The existence of the right of access to their Personal Data
- The right to rectify the Data if inaccurate or processed unfairly
- The right for their data to be deleted
- Any other information which is necessary so that processing may be fair and the Data Subject has all the information necessary in relation to the processing of their Data.

To **fairly process Personal Data**, it must have been fairly obtained, and the Data Subject must have given consent to the processing **Or**

The processing must be necessary for one of the following reasons:

- The performance of a contract to which the Data Subject is a party
- In order to take steps at the request of the Data Subject, prior to entering into a contract
- Compliance with a legal obligation, other than that imposed by contract
- To prevent injury or other damage to the health of the Data Subject
- To prevent serious loss or damage to the property of the Data Subject
- To protect the vital interests of the Data Subject, where it is inappropriate to get their consent
- Where seeking the consent of the Data Subject is likely to result in their interests being damaged
- For the administration of justice
- For the purpose of the legitimate interests of *Business to Arts*, except where the processing is unwarranted in any particular case, by reason of prejudice to the fundamental rights and freedoms and legitimate interests of the Data Subject.

To **fairly process Sensitive Personal Data**, it must be fairly obtained and the Data Subject must give explicit consent (or where they are unable to do so for reasons of incapacity or age, explicit consent must be given by a parent or legal guardian) to the processing, **Or**

The processing is necessary for one of the following reasons:

- For the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the Data Protection Officer in connection with employment
- To prevent injury or other damage to the health of the Data Subject or another person
- To prevent serious loss or damage to property
- To protect the vital interests of the Data Subject or of another person in a case where, consent cannot be given, or the Data Protection Officer cannot reasonably be expected to obtain consent
- For the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights
- For the purpose of the assessment or payment of a tax liability
- In relation to the administration of a Social Welfare scheme
- The information being processed has been made public as a result of steps deliberately taken by the Data Subject.

2.3 Only keep personal Data for one or more specified, explicit and lawful purpose(s)

To comply with this rule, staff that process Personal Data should be aware:

- That a person should know the specific reason/s why information is being collected and retained
- That the purpose for which the information is being collected is a lawful one
- They are aware of the different categories of Data which are held and the specific purpose for each.

2.4 Process Personal Data in ways compatible with the purpose for which it was given

- Personal Data should only be used and disclosed in ways that are necessary or compatible with the original purpose for which it was obtained
- Staff are not to disclose any Personal Data to any third party without the consent of the Data Subject (see Permitted Disclosures of Personal Data below)
- Personal information should not be disclosed to work colleagues unless they have a legitimate interest in the Data in order to fulfill official employment duties.

Permitted Disclosures of Personal Data:

Personal Data may be disclosed without the express written consent of the Data Subject in the following circumstances:

- Where the Data Subject has already been made aware of the person/organisation to whom the Data may be disclosed
- Where it is required by law
- Where it is required for legal advice or legal proceedings, and the person making the disclosure is a party or a witness
- Where it is required for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State

- Where it is required urgently to prevent injury or damage to health, or serious loss of or damage to property

2.5 Keep Personal Data Safe and Secure

Business to Arts promotes high standards of security for all Personal Data. The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the Data in question. Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of the Data and against their accidental loss or destruction. *Business to Arts'* standards of security include the following:

- Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractors
- Access to any Personal Data within *Business to Arts* is restricted to authorised staff for legitimate purposes only
- Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information
- Non-disclosure of personal security passwords to any other individual (including other employees in *Business to Arts*)
- Information on computer screens and manual files to be kept out of sight from callers to our offices
- Back-up procedures in operation for information held on computer servers, including off-site back-up
- Personal Manual Data is to be held securely in locked cabinets, locked rooms, or rooms with limited access
- Special care (including encryption) must be taken where mobile computing (including the electronic transfer of Personal Data via e-mail) and storage devices, such as laptops or USB's are used
- Personal Data is not to be stored on portable devices except in essential circumstances. Where deemed essential, the Data must be encrypted. Arrangements are to be in place to fully delete the Data on the portable device when it is no longer being used
- All reasonable measures are to be taken to ensure that staff are made aware of *Business to Arts'* security measures, and comply with them
- All waste papers, printouts etc. to be disposed of appropriately

2.6 Keep Personal Data accurate, complete and up-to-date

Business to Arts endeavours to meet its duty of care to the people we support and to staff by maintaining records of personal information which are accurate, complete and up-to date. In addition, it is in the interests of *Business to Arts* to ensure that accurate Data is maintained for reasons of efficiency and effective decision-making. Therefore, it is important that:

- Manual and computer procedures are adequate to maintain high levels of Data accuracy
- Staff should regularly audit their files to ensure that information is accurate and up to date
- Appropriate procedures are in place, including an annual review to ensure that Data is kept up-to-date
- Where a Data Subject informs or advises of any errors or changes to their Data, that it is amended accordingly, and as soon as reasonably possible

2.7 Ensure that Personal Data is accurate, relevant and not excessive

- Only information necessary for the stated purpose should be collected, nothing more
- A quarterly review should be carried out by managers, to examine the relevance of the Personal Data sought from Data Subjects, through the various channels by which information is collected i.e. check to confirm that questions asked on forms are appropriate, etc.
- Quarterly reviews should take place of any Personal Data already held, to make sure it is adequate, relevant and not excessive for the purpose for which it was collected.

2.8 Retain Personal Data no longer than is necessary for the specified purpose or purposes

- Staff are to be clear about the length of time that Data will be kept and the reason why the information is being retained
- Generally, Personal Data collected for one purpose, should not be retained once that purpose has ceased
- Exceptions may apply from specific legislation which require information to be retained for particular periods
- Personal Data should be disposed of securely when no longer required.
- The method should be appropriate to the sensitivity of the Data. Shredding is appropriate in respect of Manual Data; and reformatting or overwriting in the case of Electronic Data
- Particular care is to be taken when PC's or laptops are transferred from one person to another, or when being disposed of.

2.9 Provide a copy of his/her Personal Data to any individual, on request

On making a written request under Section 4 of the Data Protection Acts, any individual about whom an organisation, including Business to Arts, keeps personal information on computer, or in a Relevant Filing System, is entitled within 40 days to:

- A copy of the Data being kept about him/her;
- Know the purpose(s) for processing his/her Data
- Know the identity of any third parties to whom the Foundation discloses the Data
- Know the source of the Data, unless this would be contrary to public interest
- Be informed of the logic involved in processing the Data, where the processing by automatic means of the Data has/is likely to constitute, the sole basis for any decision significantly affecting him/her
- Know the reasons involved in decisions made about the Data Subject
- Receive a copy of any Data held in the form of opinions expressed about the individual, except where such opinions were given in confidence
- Clearly outlined reasons for an access refusal.

To make an access request the Data Subject must:

- Apply in writing (which may be via email helen@businesstoarts.ie)
- Give any details which might be needed to help identify him/her and locate the information kept about him/her

Other rights under GDPR:

- Right to have any inaccurate information rectified or erased
- Right for all data to be deleted
- Right to have Personal Data taken off a mailing list
- Right to complain to the Data Protection Commissioner

2.10 Consent to Photographs/Video/Audio Recordings

- Any photograph, video or audio recording of a person constitutes their Personal Data and is therefore, subject to the provisions of the Data Protection Acts
- In all instances where a photograph is taken, a video or audio recording is made, the explicit consent of the person and/or their parent/guardian/advocate should be sought for its use or publication in any medium
- Corporate Patrons, Members, Arts Affiliates, award entrants, artists/arts organisations and programme participants (or participants' parents and/or guardians) will be routinely asked for their permission to use their names and/or photographs on the *Business to Arts* website or other promotional material. This permission will be in written form
- The people we support, their parents/guardians/advocates are permitted to take photographs or make video/audio recordings for their own personal use, for example at concerts or award events etc.

PART 3: Compliance Audits & Data Protection Assessments (Risk Management)

3.1 Accountability & Internal Compliance Audit

Accountability requires Business to Arts to show how we are complying witht the data protection principles. This allows Business to Arts identify any risks or possible contraventions of the legislation:

- Annual Internal Compliance Audits will be undertaken by the Data Protection officer in order to identify existing and potential risks. This will take place in June each year.
- Internal Compliance Audits will review both manual and electronic data procedures and compliance
- Whilst Internal Compliance Audits will be primarily questioned based and addressed to the Head of Division and/or the Manager, a random sample of records will be examined to ensure that good practice is in evidence
- The majority of the questions in the questionnaire will be typically structured around the Seven Data Protection Principles, and *Business to Arts'* Records Management Policy
- Immediate remedial action may be prescribed by the Data Protection Officer in order to ensure that the requirements of the Data Protection Acts are observed

3.2 External Compliance Audit

External Compliance Audits of all aspects of Data protection within *Business to Arts* may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

PART 4: Data Breach Management

4.1 Introduction

A Data breach may happen for a number of reasons, including:

- Loss or theft of equipment on which Data is stored

- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error e.g. misaddressing an email
- Unforeseen circumstances such as a flood or fire
- Computer hacking
- Access where information is obtained by deception (e.g. 'social engineering' where a person in conversation, extracts confidential information from another, without having an entitlement to that information)

4.2 Management of a Data Breach in Business to Arts

There are three elements to managing a Data breach:

1. Incident Details
2. Notification of Data Breach & Risk Assessment
3. Evaluation and Response

4.2.1 Incident Details

Details of the incident should be recorded accurately by the reporter of the incident, including:

- Date and time of the incident
- Date and time it was detected
- Who reported the incident and to whom it was reported
- Description of the incidentThe type of Data involved and how sensitive it is
- The number of individuals affected by the breach
- Was the Data encrypted?
- Details of any Information Technology (IT) systems involved
- Corroborating material

4.2.2 Notification of Data Breach & Risk Assessment

Internal Notification

- A Data breach must be reported without delay to the Data Protection Officer with the Incident Details
- The Data Protection Officer will assess the incident details and the risks involved, including:

  - What type of Data is involved?
  - How sensitive is the Data involved?
  - How many individuals' Personal Data are affected by the breach?
  - Were there protections in place e.g. encryption?
  - What are the potential adverse consequences for individuals and how serious or substantial are they likely to be?
  - How likely is it that adverse consequences will materialize?

External Notification

- It is best practice to inform the Office of the Data Protection Commissioner (ODPC) immediately. (This allows the ODPC to advise, at an early stage, on how best to deal with the aftermath of a Data breach, and also to ensure that there is no repetition. It also allows the ODPC to reassure

those who may be affected by a Data breach that the ODPC is aware of it and that *Business to Arts* is taking the issue seriously).

- The Data Protection Officer will be responsible for contacting the ODPC at 1890-252-231 or info@dataprotection.ie to inform them of the Data breach.
- The Data Protection Officer in consultation with the Office of the Data Protection Commissioner (ODPC), will decide in the particular circumstance, if it is appropriate to inform the persons whose Data has been breached. In this regard, *Business to Arts* will be aware of the dangers of 'over notifying', as not every incident will warrant notification
- When notifying individuals, the DBMT will consider the most appropriate medium for doing so. It will bear in mind the security of the medium for notification and the urgency of the situation. Specific and clear advice will be given to individuals affected by the Data breach, on the steps they can take to protect themselves and, what *Business to Arts* is willing to do in order to assist them. *Business to Arts* will also provide a contact person for further or ongoing information.
- The Data Protection Officer will also consider notifying third parties, such as An Garda Síochána, bank or credit companies who can assist in reducing the adverse consequences to the Data Subject.

4.2.3 Evaluation & Response

Subsequent to any data/information security breach, a thorough review of the incident will be made by the Data Protection Officer. The purpose of this review will be to:

- Ensure that the steps taken during the incident were appropriate
- Describe and record the measures being taken to prevent a repetition of the incident
- Identify areas that may need to be improved
- Document any recommended changes to policy and/or procedures which are to be implemented as soon as possible thereafter.

PART 5: Awareness Training & Support for Staff who process Personal Data

5.1 Introduction

Business to Arts endeavours to support staff members who process Personal Data, through Data Protection Awareness Training and Data Protection Support mechanisms.

5.2 Data Protection Awareness Training

Data Protection Awareness Training will take place during induction of new staff, and at various intervals throughout an employee's professional career in *Business to Arts*.

5.3 Data Protection Support

Data Protection Support is provided by the Data Protection Officer

CONCLUSION

This Policy will be reviewed on an annual basis or earlier if appropriate, to ensure it remains comprehensive, current with legislation, and relevant to good practice.

Helen Carroll
Data Protection Officer

25 May 2018

Approved by the Board of Business to Arts