Data Protection Policy

Status: Live
Version: 1.3
Date: 10 November 2018

Bristol Multi Faith Forum

Contents

Introduction

This document

This document contains the BMFF policies relating to data protection, including personal data protection and data privacy. Details of the data itself can be found in the BMFF Data Register, which can be found on our web site.

Definitions

Within this document, the following terms and abbreviations should be understood as described below.

- **BMFF**: Bristol Multi Faith Forum.
- **DC**: Data Controller. The Steering Group is the BMFF DC.
- **DP**: Data Processor. A BMFF worker, paid or voluntary, who who has agreed to and been trained to process personal data on behalf of the BMFF: they may collect, store, use, correct or delete personal data. Different DPs may be authorised and empowered to undertake different kinds of data processing, or to undertake data processing on different categories of data.
- **DPIA**: Data Protection Impact Assessment. This is a process to help us identify and minimise the data protection risks of a project (see the relevant section bellow).
- **DPO**: Data Protection Officer. A member of the Steering Group who takes a special interest in and responsibility for data protection (one aspect of which is data privacy) and who handles the day to day data protection activities.
- **DS**: Data Subject. An individual whose data we hold.
- **SAR**: Subject Access Request.

Summary

We comply with all relevant legislation concerning personal data; we provide appropriate training to our Steering Group (the DC) and to our workers, paid or voluntary, to ensure that they all know their responsibilities and are able to function accordingly. We will take measures to address any problems with the policies and procedures, or with their implementation, as soon as possible, once we become aware of them.

Questions about our policies and procedures in this area should be directed in the first instance to the DPO. Any identified problems should be communicated as soon as possible to the Chair of the Steering Group or the DPO.

Personal Data

Collection

When personal data is collected from individuals, we will inform them why their data is being collected and how it will be used; we will also provide them with access to our Data Privacy Statement, Data Register and full Data Protection Policy.

When personal data is collected at an event through the use of a sign-up sheet, we will provide alongside the sign-up sheet the text of our Data Protection Summary (available in our Data Privacy Statement), which will also inform people of more secure ways they can provide their information. The sign-up sheet will be held securely by a DP and saved in the appropriate data store at the earliest opportunity. Once the data has been stored and backed up, the original sign-up sheet will be destroyed.

When personal data is collected through a commercial relationship, only data which is relevant to the functioning of that relationship will be collected.

Security

We make every reasonable effort to maintain the security of the data we hold.

Passwords to secure the data will not be used elsewhere, and will be changed if there is any suspicion that they have been compromised.

Special Category Data

Special Category Data is broadly similar to the 'sensitive personal data' category recognised by the Data Protection Act (1998). Information about a person's religion is one type of Special Category Data.

We must have a lawful basis for processing Special Category Data, in exactly the same way as for any other personal data. The difference is that we also need to satisfy one or more of the specific conditions listed under Article 9 of the GDPR.

We hold information about religion under condition (e) of Article 9(2): processing relates to personal details which are manifestly made public by the data subject.

Subject Access

Responsibility for responding to a SAR lies in the first instance with the Development Worker. If the Development Worker cannot respond (if they are on holiday or sick, for example) then the responsibility passes to the DPO. We aim to respond to every SAR as soon as possible, and in any case within two weeks of receiving the request.

When a SAR is received by email and the email address is the same as the email address we have on record for the individual requesting their data, we will send the information by email to that address.

When a SAR is received in some other way, then the identity of the person making the request and the format in which the information is required will be verified before responding: this is to ensure that we do not accidentally send personal information about one person to someone else.

Correction

We will correct personal data if requested by the DS. If someone other than the DS makes the request, we will verify with the DS that this is a correct request before making the change.

If the data correction request is given to a BMFF worker who is not a DP, they will pass the request to a DP at the earliest opportunity; the DP will make the change and confirm it to the worker; if the worker has a copy of the personal data, upon receiving this confirmation, they will immediately delete or destroy it.

Upon receiving a request to correct personal data, and verifying the request if necessary, the DP will make the change and then confirm to the DS that the change has been made.

Deletion

The procedure for deletion of personal data is essentially the same as the procedure for correction, described above, with the following additions.

We will ask the DS why they are asking to be deleted, if this information has not been provided. Details of the number of deletions and the reasons given will be provided to the Steering Group at the time of the annual data clean-up, or more frequently if appropriate.

Deletion consists of flagging the record of the DS as ‘deleted’ and adding the deletion date and the reason for deletion (if provided). Some personal data may also be removed from the database, but sufficient will be retained to enable BMFF to identify that this individual has been deleted and their faith community. There are several reasons for this: one is to ensure that nobody, looking at the database at some time in the future spots that this person is not present and invites them to join; another is to ensure that proper and accurate analysis of event attendance can be undertaken.

Data Breach

A data breach may be unknown, suspected or confirmed.

If we know nothing about a data breach, we will be unable to do anything about it. If someone involved with BMFF becomes aware of a data breach, they have an obligation to notify the Chair or DPO.

A data breach will be suspected if it is discovered that data security has not been maintained: for example, if a laptop with the data is lost, or if it is left unlocked and unattended in a public place.

It will be hard to confirm an actual data breach, unless the person responsible

admits to what they have done and provides evidence.

In the event of a suspected or confirmed data breach, we will:

- investigate the situation;
- decide on the appropriate response; and then
- contact the people affected and inform them of the situation and what we are doing about it.

Data Transfer

We do not transfer any data to another country, or supply it to another organisation or individual. We do not give, sell or provide access to the data we hold.

We sometimes agree to send out information on behalf of another organisation, if it fits within the scope of the information our contacts have agreed to receive. In this situation, we receive the information and send it out to our contacts: our contact details are never provided to the other organisation.

Data Subjects' Rights

We recognise the rights of each of our Data Subjects to own their data and exercise control over it.

They are able to withdraw any consent they have given at any time: we will ask why they are withdrawing consent, to enable us to understand what is happening and if possible provide a better service as a consequence, but nobody will be required to provide a reason when they withdraw consent.

Automated Processing

We do not undertake any automated processing of personal data.

Data Protection Impact Assessment ('DPIA')

Summary

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project. We must do a DPIA for certain listed types of processing (itemised below), or any other processing that is likely to result in a high risk to individuals' interests. Following good practice advice, we will also do a DPIA for any other major project which requires the processing of personal data.

To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals: high risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We keep our DPIAs under review and revisit them if necessary.

Mandatory screening checklist

We always carry out a DPIA if we plan to do one of the following activities.

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.
- Change the nature, scope, context or purposes of our processing.

Optional screening checklist

If we plan to carry out any of the following activities, we will consider carrying out a DPIA; if we decide not to carry out a DPIA we will document our reasons:

- evaluation or scoring;
- automated decision-making with significant effects;
- systematic processing of sensitive data or data of a highly personal nature;
- processing of data on a large scale;
- processing of data concerning vulnerable data subjects;
- adopting innovative technological or organisational solutions;
- processing involving preventing data subjects from exercising a right or using a service or contract; or
- any major project involving the use of personal data.

Process checklist

A DPIA will normally include the following activities.

- We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

- We ask for the advice of our data protection officer.
- We describe the nature, scope, context and purposes of the processing.
- We identify and undertake an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
- We ask our data processors to help us understand and document their processing activities and identify any associated risks.
- We identify any measures we can put in place to eliminate or mitigate those risks.
- We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.
- We record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- We consult the ICO before processing if we cannot mitigate high risks.
- We implement the measures identified, and integrate them into our project plan.

Contracts with data processors

Contracts with all data processors will contain the following terms.

In the following, 'data' means the personal data you have access to through the BMFF and the personal data you process on behalf of the BMFF; 'Data Subjects' are the people to whom that data relates.

- You have a duty of confidence towards us and towards any and all Data Subjects whose data you have access to.
- You will ensure that the data is only held in the data stores identified in the BMFF Data Register.
- You will handle all data in accordance with our Data Protection and Confidentiality policies.
- You will only use data in accordance with written instructions by the Data Controller, unless required by law to act without such instructions.
- You must take appropriate measures to ensure the accuracy and security of all data.
- You are not allowed to engage a sub-processor: if one is needed, they will be engaged by the Data Controller.
- You must assist the Data Controller in providing subject access and allowing data subjects to exercise their rights under the General Data Protection Regulations.
- You must notify the Data Protection Officer as soon as possible after you discover or suspect a data breach.
- You may be required to assist the Data Protection Officer with any Data Protection Impact Assessment which is undertaken.
- You may be subject to investigative and corrective powers of a supervisory

authority (such as the ICO) under Article 58 of the General Data Protection Regulations, and you must cooperate with them if requested.

- You must delete or return all personal data to the Data Controller at the end of the contract.
- The Data Controller and Data Protection Officer are both able to undertake or instigate audits and inspections of the data and data processing; you must fully comply with any such audits or inspections and do whatever else is within your power to ensure that we comply with all our legal obligations of whatever kind.
