Bristol Raceway Ministries
P.O. Box 1414 Bristol, TN 37621
(423) 430-0798
EIN 20-3447387

Bristol Raceway Ministries
Information Collection and Data Storage Policy

1. Introduction to the Policy

Bristol Raceway Ministries (hereafter referred to as "We"/"Us") uses personal data about living individuals for the purpose of general ministry administration and communication.

We recognize the importance of the correct and lawful treatment of personal data. All personal data, whether it is held on paper, on a computer, or other type of media, will be subject to the appropriate legal safeguards and good practice as specified in the General Data Protection Regulation 2018.

We fully endorse and adhere to the eight principles of the GDPR and value your privacy. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Volunteers and any others who obtain, handle, process, transport, and store personal data for us must adhere to these principles.

2. At A Glance

What information is being collected?

We collect information such as your name, contact details, and age.

Who is collecting it?

Bristol Raceway Ministries

How is it collected?
The information is collected by the completion of forms or electronic submission of data by the person the data relates to.

Why is it being collected and how will it be used?

For general ministry administration, for communication with you (if you agree).

Who will it be shared with?

Our board of directors, and secretary, but never with anyone else. You can also choose to share your information with other members of the ministry, but this is up to you.

How will it affect you?

If you agree by providing consent, you will receive email, text messages, and or phone calls from us.

3. The GDPR Principles

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant, and not excessive for those purposes.
4. Be accurate and where necessary, kept up to date.
5. Not be kept for longer than is necessary for that purpose.
6. Be processed in accordance with the data subject's rights.
7. Be kept secure from unauthorized or unlawful processing and protected against accidental loss, destruction, or damage by using the appropriate technical and organizational measures.
8. Not be transferred to another country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Your Rights

The rights of the data subject are:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object; and
- The right not to be subject to automated decision-making including profiling.

4. Maintaining Confidentiality

We will treat all your personal information as private and confidential and will not disclose any data about you to anyone other than the board of directors, and secretary in order to facilitate the administration and day-to-day communication within the ministry, unless you request otherwise.

All board of directors, general officers, and volunteers who have access to Personal Data will be required to sign a Data Protection Understanding and Acceptance form once they do their annual Data Protection Training as well as read the Data Protection Policy.

We will never sell your data or share it with any external third party and we promise to keep your data safe and secure.

5.1. Exceptions

There are four exceptional circumstances to the above permitted by law:

1. Where we are legally compelled to do so.
2. Where there is a duty to the public to disclose.
3. Where disclosure is required to protect your interest.
4. Where disclosure is made at your request or with your consent.

5.2. Use of Personal Information

We will use your data for three main purposes:

1. The day-to-day administration of the ministry, e.g., maintaining financial records of giving for audit and tax purposes.
2. Contacting you to keep you informed of ministry activities and events.

6. Storage of Data

6.1. The Database

Information contained in the database will not be used for any other purposes than set out in this section. The database is accessed through the internet and therefore, can be accessed through any computer or smart device with internet access. The server for the database is in the United States and hosted by Google.

6.1.1. Access to the database is strictly controlled through the use of name-specific passwords, which are selected by the individual.

6.1.2. Those authorized to use the database only have access to their specific area of use within the database. This is controlled by the Data Controller and other specified administrators. These are the only people who can access and set these security parameters.

6.1.3. People who will have secure and authorized access to the database include the executive director, our secretary, and our financial comptrollers. Anyone with access to the database is required to complete the Data Protection Understanding and Acceptance form.

6.1.4. The database will NOT be accessed by any authorized users outside of the U.S. or E.U., in accordance with the Data Protection Act, unless prior consent has been obtained from the individual whose data is to be viewed.

6.1.5. Subject Access - all individuals who are the subject of personal data held by Bristol Raceway Ministries are entitled to:

- Ask what information the ministry holds about them and why.
- Ask how to gain access to it.
- Be informed on how to keep it up to date.
- Be informed what Bristol Raceway Ministries is doing to comply with its obligations under the 2018 General Data Protection Regulation.

6.1.6. Personal information will not be passed onto any third parties outside of the ministry, other than listed under the "Maintaining Confidentiality" section.

6.1.7. Subject Consent - The need to process data for normal purposes has been communicated to all data subjects. In some cases. If the data is sensitive, for example, information about health, race, or gender, express consent to process the data must be obtained.

6.2. Other Storage

Occasionally, data needs to be stored outside of the Database. This includes the written consent for data to be used and processed, and forms filled out by the information owner to update the database. On these occasions, it will be stored electronically and/or physically.

6.2.1. Electronic data outside of the Database will be stored on the cloud, specifically Google Drive to which all principles laid out in **6.1** apply.

6.2.2. Physical Data will be stored in a locked filing cabinet in a locked office on the ministry premises. People who will have secure and authorized access to the data include the executive director, our secretary, and our financial comptrollers.

6.2.3. Data should not and will not be stored on authorized person's personal computers or devices, or at any address other than the ministry office.

7. Rights to Access Information

Volunteers and other subjects of personal data held by Bristol Raceway Ministries have the right to access any of their own personal data that is being held in certain manual filing systems. This right is subject to certain exemptions: Personal Information may be withheld if the information relates to another individual.

Any person who wishes to exercise this right should make the request in writing to Bristol Raceway Ministries, using the address which is available in the header of this page.

If personal details are inaccurate, they can be amended upon request, or by the data subject if held on the Database.

Bristol Raceway Ministries aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 30 days of receipt of a completed form unless there is a good reason for delay. In such cases, the reason for the delay will be explained in writing to the individual making the request.

8. Retention of Data

8.1. Database

Data held on the Database will be held as long as the person is an active member of Bristol Raceway Ministries.

After this point, data will be either:

- Deleted immediately, if a person requests deletion.
- Archived on the database, then deleted after 6 months.

8.2. Data Retention Times

Different data will be retained for different periods of time, depending on the content. Please see the table in Appendix 2.

9. GLOO

The executive director and our secretary may use the SMS messaging service of GLOO.us to contact individuals, Individuals should be invited to participate in the group individual message, and they will have the option to opt out of receiving messages through the GLOO.us SMS message system. This enables you to have the choice as to whether you should receive future messages or not thus allowing them the choice of information sharing.

10. What if something goes wrong? (Data Security Breaches)

10.1. Definition

A data security breach could be caused by human error or malicious intent and its definition is “any loss of or unauthorized access to Bristol Raceway Ministries data”.

Examples of data security breaches may include:

- Unauthorized access to confidential data
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking attack
- Offences where information is obtained by deceit

10.2. Response

Bristol Raceway Ministries response to a data security breach will be as follows:

- Report – the person who discovers the breach will report it promptly to the executive director. The report should be in writing (usually by email) and should include full and accurate details of the incident including who is reporting the incident and the type of data involved, using the Data Breach Incident Report Form in Appendix 3 if possible.
- Assess – an assessment will be made to establish the severity of the breach and to ascertain who will lead in the management of the breach.
- Contain and Recover – action will be taken to ensure whether anything can be done to prevent further loss/breach, recover losses, and limit any damage that may be caused.
- Inform – any person whose personal data has been breached will be informed, if appropriate.
- Evaluate and Respond – an evaluation will be taken to establish if any present or future risks apply, and any findings will be acted upon and implemented to prevent future data security breaches.

Key details

Policy Prepared by: Ellis Bishop, Executive Director
Originally Approved by the board of directors on: 3/10/2024
Last Reviewed on: 3/10/2024
Next review date: 3/10/2026