CROSSROADS BIBLE CHURCH

PERSONAL DATA PROTECTION POLICY

PL005 Ver. 2023.01

BRIEF DESCRIPTION

The purpose of this document is to establish the practices that we have implemented in the organization in relation to the handling of personal data, from its collection, storage, its use and with whom we share that information.

Tablea of contents

Our goal is the protection of your data

At CROSSROADS BIBLE CHURCH we recognize the importance of privacy and the sensitivity of the information we keep in our database, especially personal information about people who visit us, whether or not they are members of the organization, as well as collaborators, suppliers or others.

As a religious and Christian formation organization, we have a moral, ethical, and legal obligation to keep all information we receive confidential as part of our church-believer relationship. Additionally, we are committed to safeguarding the information that we store and/or process about people, whether natural or legal.

In this Data Protection Policy, hereinafter "Policy", we establish the practices that we have implemented in the organization in relation to the handling of your data, from its collection, storage, its use and with whom we share such information.

To whom this Policy applies

This policy applies to us, as the custodian of the database and as the controller of your personal data, and to you, the natural person, as the owner of the data.

When we say “We”, we mean “CROSSROADS BIBLE CHURCH” hereinafter the organization.

When we say "You," we mean you as a visitor, member, collaborator, volunteer, supplier or person who for any reason shares your personal data with us.

Legal Basis of this Policy

This Policy is based on Law 81 of March 26, 2019 on the Protection of Personal Data, which seeks to protect the rights of natural persons in their capacity as owners of their personal data, regarding the use of these data, and Executive Decree 285 of May 28, 2021 that regulates it.

Law 81 applies to all databases located in the territory of the Republic of Panama, when they store personal data of nationals or foreigners, or when the data controller is domiciled in the Republic of Panama. The databases of subjects regulated by special laws are excepted provided that these laws establish minimum technical standards necessary for protection equal to or greater than those established by Law 81.

Definitions

Below we detail some concepts or definitions offered by Law 81 for the terminology that we use in this policy.

Typo of data

- Personal data. Any information concerning natural persons, which identifies them or makes them identifiable.
- Confidential data. Those data that by their nature should not be public knowledge or unauthorized third parties, including those that are protected by law, by confidentiality or non-disclosure agreements, in order to safeguard information. In the cases of the Public Administration, they are those data whose treatment is limited for the purposes of this administration or if there is the express consent of the owner, without prejudice to the provisions of special laws or regulations that develop them. Confidential data will always be restricted access.
- Sensitive data. That which refers to the intimate sphere of its owner, or whose improper use may give rise to discrimination or entails a serious risk for it. By way of example, personal data that may reveal aspects such as racial or ethnic origin are considered sensitive; religious, philosophical and moral beliefs or convictions; union membership or political opinions; data related to health, life, sexual preference or orientation, genetic data or biometric data, among others, subject to regulation and aimed at uniquely identifying a natural person.

Storage

- Data storage. Conservation or custody of data in a database established in any provided medium, including Information and Communication Technologies (ICTs).
- Database. Sorted set of data of any nature, whatever the form or modality of its creation, organization or storage, which allows the data to be related to each other, as well as any type of treatment or transmission of these by its custodian.
- Accessible source. Databases that are not of restricted access or contain any reservation to consultations, or that are of public access, such as official state publications, the media, telephone directories and the list of people who belong to a group of professionals that contain only name, title or profession, activity, work or commercial address, as well as information that indicates their belonging to organizations.

Participants

- Owner of the data. Natural person to whom the data refer.
- Custodian of the database. Natural or legal person, of public or private law, lucrative or not, that acts in the name and on behalf of the data controller and is responsible for the custody and preservation of the database.
- Data controller. Natural or legal person, public or private law, lucrative or not, that is responsible for decisions related to data processing and that determines the purposes, means and scope, as well as issues related to these.

Data processing

- Data processing. Any operation or complex of operations or technical procedures, automated or not, that allows the collection, storage, recording, organization,

elaboration, selection, extraction, confrontation, interconnection, association, dissociation, communication, assignment, exchange, transfer, transmission or cancel data, or use it in any other way.

- Consent. Manifestation of the will of the owner of the data, through which the treatment of these is carried out.
- Data blocking. Temporary restriction of any access or processing of stored data.
- Cancellation or deletion of data. Delete or permanently delete the data stored in databases, whatever the procedure used for it.
- Expired data. That data that has lost validity by provision of the law, due to the fulfillment of the condition or the expiration of the term indicated for its validity or, if there is no express rule, due to the change of the facts or circumstances that it records.
- Modification of data. Any change in the content of data stored in databases.
- Dissociation or anonymization procedure. All data processing that prevents the information available in the database from being associated with a specific or determinable natural person.
- Data transfer. Disclose, divulge, communicate, exchange and/or transmit, in any way and by any means, from one point to another, intra or extra-border, the data to natural or legal persons other than the owner, whether determined or indeterminate.

The Principles that Guide us

As an organization we adhere to the following principles established in Law 81, namely:

- Loyalty. We obtain your personal data only with your knowledge and consent as the owner of it.
- Purpose. When we obtain your personal data we inform you about the purpose and we will only use it for the stated purposes.
- Proportionality. We will only request the necessary personal data related to the established purpose.
- Veracity and Accuracy. We will always ensure that your data is accurate and kept up to date. Remember that updating is a shared responsibility.
- Data security. We have taken appropriate technical and organizational measures against unauthorized and unlawful processing of your data and personal information. You can rest assured that we have a robust technological platform, expert advice and a specialized team that has developed a strategy to continuously optimize the security of your personal data.
- Transparency. We will always try to communicate our data protection policies in a language that is easy to understand. See also the sections We take care of your Rights as the Owner of Personal Data and Access to Your Information and Procedure to exercise your rights.
- Confidentiality. All persons who, due to their role, have access to your data are obliged not to disclose them and to keep them confidential, even when their

relationship with the owner of the data or with the person responsible for processing them has ended. We have internal processes, policies and tools to support us in maintaining the confidentiality of your data.
- Lawfulness. When we obtain your data, we ensure that we have your consent and document it for future reference.
- Portability. If requested by you, we will share your personal data from time to time in a generic and common format.

How and why do we collect personal information?

As a religious and Christian formation organization, we collect personal data as part of our ministry activities and church programs in order to serve, disciple, care for, and empower our members and their families.

We never collect personal data without your knowledge and consent. We do not use your personal data for purposes other than those indicated.

It is important to note that we do not disclose or sell your personal information to third parties to enable them to market their products and services.

If you are a member, regular attendee or visitor

When you visit us for the first time or regularly, or request to be a formal member of the organization, we may collect your information and data, as part of the welcome process, registration for events, to understand, access and assist you with your needs, among others. We only collect your data through legal and consensual means.

The information we typically collect includes:

- Information and basic personal data to identify you unequivocally: full name, date of birth, nationality, passport or identification number.
- Contact information to be able to communicate with you: physical address, email address, telephone numbers.
- Information necessary to comply.

Generally, you will have provided information and data in the course of our relationship. However, as necessary, to provide ministerial services and/or comply with legal obligations, we may validate or collect information about you with our different databases, such as those of other organizations in our group, or through third parties such as accessible sources, other authorities and/or state entities and service providers.

We use your personal data only in our regular ministerial activities and to comply with our obligations in the agreements signed to provide you with our services, to comply with our

legal obligations in the jurisdictions where we operate, as well as to comply with judicial and/or administrative orders if necessary.

Due to the diversity of ministerial activities that we provide, we cannot define a general fixed term for the cancellation of the personal data that we have in our custody. We will keep your personal data for a minimum of 5 years after the termination of any contractual or ministerial relationship. We will keep your personal data after this period for as long as necessary to be able to attend to any claim or care that arises from the treatment for which they have been collected or to comply with special laws or the regulations that develop them.

As part of our ministerial relationship, we may send you information about our ministries, events, and news about our organization or other related organizations. You may at any time withdraw your consent by notifying us at dataprivacy@cbcpanama.org

If you visit us at our facilities
In our building we use video surveillance around and inside our facilities, to maintain the security of regular attendees, collaborators and other visitors, as well as to protect ourselves against theft, fraud and property damage. Therefore, when you visit us at our facilities, you can be recorded. Any recording is destroyed after a maximum of 1 year and will not be used for purposes other than those described here.

If you visit us on our Internet pages, service portals or mobile applications
If you, through our contact forms, prayer requests, registration to events, etc., provide us with your contact information to communicate with us, we will pass your data to the indicated persons to attend to your request. It is not used for any other purpose. If a relationship with you is not established, your data will be discarded after a maximum period of 6 months.

When entering one of our service portals, such as payments or donations, we collect the information that you provide us at the time and that is strictly necessary for it to fulfill the purpose for which it was designed. In all cases we always seek your comfort and the security of your data. In these cases, your data will be stored for the periods established by applicable laws and in this policy.

If you visit us on our social media accounts.
By visiting the CROSSROADS BIBLE CHURCH accounts on Facebook, Instagram and YouTube or any other, you will have accepted the Data Protection Policies of these networks. CROSSROADS BIBLE CHURCH does not collect your data or offer advice through the aforementioned social networks.

If you provide a service to us as a supplier or participate in a procurement process.

When you are our supplier or bid with us, we may ask you for general information about yourself, contact details, commercial references, references in the APC(Asociación Panameña de Crédito) and any other information that is required to carry out due diligence and assess the risk of a contractual relationship.

We will keep the personal data that you provide us in the course of our commercial relationship for a minimum of 5 years after the end of any commercial or contractual relationship. We will keep your personal data after this period for as long as necessary to be able to attend to any claim or care that arises from the treatment for which they have been collected or to comply with special laws or the regulations that develop them.

If you are an employee, volunteer or candidate for a position
When you apply for a position with us, we collect the information you provide us with your resume. In addition, we may be collecting additional information, for example through forms, interviews, or your references. We use this information in order to evaluate candidates to fill a job or volunteer position with us. If you are not hired, we keep your data for a period of 12 months and then we delete it.

If you are hired by us, your information will form part of our employee database and your personnel file, for which we may request and store additional information, in order to develop the employment relationship. Once the employment relationship has ended, we keep your data in accordance with the applicable special laws, such as Law 51 of 2005, which reforms the Organic Law of the Social Security Fund and dictates other provisions, in which a term of 20 years for the prescription of quotas, so the relevant information will be kept for at least 20 years after the employment relationship ends.

How do we share or transfer your information?

In the course of our business relationship, we provide information to our staff for ministerial management purposes. Our staff is trained to maintain the confidentiality and security of your data.

All our staff and volunteers with access to personal information of members, regular attendees or visitors have signed a confidentiality agreement and receive continuous training on confidentiality policies and protocols, data protection and our Code of Ethics, among others.

In order to carry out some of our activities we may sometimes use external service providers or professionals who work with us, such as consultants, translators, IT service providers, banks and others, who may have access to your personal data. In these cases, we require that these providers comply with practices and policies that ensure the security and confidentiality of your personal data and that they are not processed for purposes other than those previously specified.

Some of our service providers may be located in different jurisdictions. When it is necessary to transfer or transmit your personal information for the indicated purpose, we always ensure that the protection and confidentiality of your data is maintained as if it were in national territory and always in compliance with applicable regulations.

Always keep in mind that we must and will provide your data and basic information to government authorities, when it is requested and must be delivered in accordance with the law or subject to compliance with international treaties ratified by the Republic of Panama.

Information Security

The information we collect is used strictly for the stated purposes. The access of our employees and volunteer staff to your information is restricted and limited only to those who have authorization and training in the proper handling of personal data information.

We have adopted and applied physical, electronic, procedural safeguards and security practices to ensure that your information is kept confidential and secure as required by law and our internal procedures and practices.

If you have any questions about our security measures, you can contact us at dataprivacy@cbcpanama.org

Information Retention

You agree that we may maintain and use information about you in our records for the purposes described in this Policy, even if you cease to have a relationship with us, subject to applicable laws, or until you as the owner request the cancellation of your data with U.S.

Accuracy of Personal Information

As long as there is a relationship or association with us, you must at all times provide and keep all personal information updated, and you must notify us as soon as there are changes to it so that we can update our databases and ensure that there are no mishaps in the relationship we have.

We take care of your Rights as Owner of Personal Data

- Access. You can obtain your personal data, know its origin and the purpose for which it has been collected, within a period not exceeding 10 business days from the request.
- Rectification. You can request correction of your personal data, if you consider that these are incorrect, irrelevant, incomplete, out of date, inaccurate, false or

impertinent. In such a case, we will proceed with the corresponding correction within a period of 5 business days following the request.

- Cancellation. You can request the deletion of your data, if you consider that these are incorrect, irrelevant, incomplete, out of date, inaccurate, false or irrelevant. In this case, we will proceed with the corresponding cancellation within a period of 10 business days following the request.
- Opposition. When you consider that there are well-founded and legitimate reasons related to something in particular, you can refuse to provide your personal data or to subject it to certain treatment, as well as to revoke your consent. In this case, we will proceed and respond within 5 business days of the request.
- Portability. If required by you, we will share your personal data in a generic and common format, within a period of no more than 10 business days from the request.

Please note that to protect your rights we may delete, cancel, modify or block your personal data without your request, when there is evidence of inaccuracy of your data. Where the accuracy of your data cannot be established or is in doubt, we may block your data.

Access to Your Information and Procedure to exercise your rights
To exercise the rights detailed above, please send an email to our Data Protection Officer, detailing your request and with the required supporting documentation. We will respond to you within the previously indicated periods, counted in business days from the day after receiving the request.

Data Protection Officer

We have appointed a Data Protection Officer, who ensures timely attention to the owners and competent authorities based on the Personal Data Protection Law:

Data Protection Officer:	Edilberto Tapiero
Contact:	dataprivacy@cbcpanama.org
Office:	Ave. Omar Torrijos, Calle Rufina Alfaro Edificio 6582, Ciudad de Panamá

Functions of the Data Protection Officer (excerpt):

- Participate in matters related to the protection of personal data.

- Inform and advise the data controller and/or the database custodian on matters related to compliance with the Personal Data Protection Law, its regulations, or any legal provision applicable to each case.
- Supervise compliance with regulations.
- Promote the training of people who take on tasks related to the processing of personal data.
- Cooperate with the control authority and be its liaison unit.
- Advise the data controller and/or the database custodian in responding to requirements or observations formally notified by the control authority.
- Be the liaison unit with the data owners for issues related to data processing and their rights.

Validity of this Policy

This Policy was updated as of August 1, 2022. You agree that we may review and change our Policy at any time in order to update our privacy commitment to you, based on current privacy laws and best practices.
Any change to this Policy will be duly communicated within a period not exceeding 10 days from the approval of the changes made.

Personal Data Protection PolicyApproval and Revision History

The history of approval and review of the Personal Data Protection Policy is documented in the following tables:

Approval

Originator	Reviewer	Approver
Ricardo Chang		CROSSROADS BIBLE CHURCH's Leadership Team

Revision History

Revision	Date	Originator	Summery of Changes
Ver.2023.01	08/01/22	Ricardo Chang	