CROSSROADS
INTERNATIONAL CHURCH OF BASEL

Data Protection Policy

Version 19.4, definite version 2019

1. Context and overview

1.1 Key details

- Policy prepared by: Nico Hoogenraad, Associate Pastor
- Approved by Elder board on: August 22nd, 2019
- Policy became operational on: October 1st, 2019
- Next review date: August 2022, or sooner if Swiss law requires

1.2 Introduction

Crossroads International Church of Basel (hereafter: Crossroads) needs to gather information about individuals - mostly about members, vendors, attenders and other interested individuals with whom Crossroads has a relationship.

This policy describes how this personal data will be collected, handled and stored to meet the organization's data protection standards and comply with the law.

1.3 Why this policy exists

This data protection policy ensures that Crossroads:

- Complies with Swiss and European data protection law and follows good practice
- Protects the rights of staff, members, attenders, vendors and interested individuals
- Is open about how it collects, stores and processes individuals' data
- Protects itself from the risk of a data breach

1.4 Data protection law

Crossroads is a Swiss organization - a 'Verein' - and collects, stores and uses the data it collects within Switzerland. Therefore, Swiss legislation on data protection is applicable. At the time of writing this policy it is the Federal Act of Data Protection of June 19th, 1992 and the Ordinance to it of June 14th, 1993. However, Switzerland is preparing updated legislation in line with the European GDPR that is expected to be put into effect in 2019.

However, Crossroads also processes information on members, attenders, vendors and other interested parties residing in France, Germany and perhaps other European countries, and therefore there is a strong argument that alongside the applicability of Swiss data protection laws, the GDPR (General Data Protection Regulation) of the European Union is also applicable, which Regulation has been in effect since May 2018.

1.4.1. Principals of Data Protection

In GDPR and in the expected amended Swiss data protection laws, the framework is laid for how organizations have to protect the third-party information that they hold in the context of their operations. In order to prevent data loss, organizations need to protect the information by taking technical and organizational measurements. They have to use modern techniques to protect digital personal information, while also being prudent about how the organization handles this information, who has access to the information, and what is done with it.

Organizations are required to think about the safety of the information before they start collecting data. Subsequently, they need to give continued attention within the organization to keeping data up-to-date and sufficiently protected in the light of technological developments.

Some of the areas of attention in the legislation are:

- Transparency, appropriateness, legality, accuracy
- Processing only what is necessary
- Confidentiality
- In-house security
- Security when processed by third parties
- Measurements in a plan-do-check-act cycle
- Measurements based on risk analysis
- Measurements based on security standards
- Agreements for processing by third parties
- Reliability requirements
- Evaluation and adjustments

1.4.2. Notification of data leaks

GDPR, stipulates that, in the case of a data leak of personal information, the organization has to report this to the appropriate authorities. In the 1992 Swiss data protection law, there is no such reporting requirement, but it is expected that there will be such an obligation in the updated data protection law.

Recording and storing personal information from individuals from multiple European countries (at least Germany and France), additional to the recording and storing of personal information on people residing in Switzerland, might require Crossroads to report this to multiple authorities in the event of a data breach. As this is superfluous in light of the limited number of European residents, we will assume that reporting a data leak to the Swiss authorities suffices, once this obligation has been put into effect in the new law that will be passed. The underlying assumption is that residency determines which law is applicable and not the fact that Swiss residents may in many cases be EU subjects. As most people whose personal information we process reside in Switzerland, we conclude that Swiss law has to prevail, but we will reckon with European GDPR where we can.

A data leak is defined as access, destruction, modification or release of personal information, without it being the intention of the organization. Unlawful processing is also considered to be a data leak. With a data leak, personal information has been subject to loss or illegal processing – things that security measures should have prevented. This includes loss of USB sticks, a stolen laptop or unwanted access to data files by a physical or digital hacker.

1.4.3. Notification of data leaks to the Authority

The Authority supervises compliance of privacy legislation on registration of personal information. When a data leak is discovered, the organization has to report this to the Authority. Within the organization, it should be clear who will report a data leak to the Authority. In the context of Crossroads, this is the Senior Pastor. Because we first and foremost follow Swiss law, the notification of data leaks to authorities only becomes appropriate once updated, applicable Swiss law is put into effect.

2. People, risks and responsibilities

2.1 Policy scope

This policy applies to:

- Crossroads office in Basel and the employed Church Staff

- The Elder Board of Crossroads, which is the governing body and responsible for oversight of the implementation of this policy
- All volunteers of Crossroads that carry out tasks and responsibilities within the organization of whatever kind
- All individuals and organizations that Crossroads uses or might use – paid or unpaid - to process or analyse the personal information of individuals, including outside payroll companies which process payroll for employees, insurance companies, etc.

It applies to all data that Crossroads collects and holds relating to identifiable individuals and can include:

- Names of individuals
- Postal and/or physical addresses
- Email addresses
- Telephone numbers
- Donation information
- Way of involvement with Crossroads
- Attendance at Crossroads meetings, whether Sunday services, home group meetings or other
- Notes on pastoral care (classified)
- Salary payments and personnel files

2.2 Data protection risks

The risks that Crossroads might assume with personal information are summarized as follows:

- **Breaches of confidentiality.** For instance, the giving information of individuals becomes known to people that do not need to know
- **Failing to offer choice.** For instance, individuals should be able to indicate they do not want Crossroads Compass emails, even though they are members
- **Theft.** For instance, hackers tap into the Elvanto database and publicize the list of names on the Internet, or an Elvanto user uses the emails of individuals to send them direct marketing about another Christian organization
- **Reputational damage.** For instance, Crossroads' reputation will be damaged if personal data becomes available in ways Crossroads did not intend

2.3 Responsibilities

Everyone that works for Crossroads, whether paid or as a volunteer, has some responsibility for ensuring data safety. However, the following people have key areas of responsibility:

- The **Elder Board** is ultimately responsible for ensuring that Crossroads meets its legal obligations, and needs to approve any new or updated data protection policies
- The **Administrative Assistant** functions as the responsible officer for the database and ICT security and is responsible for:
    - Keeping the Senior Pastor updated about ICT and data protection responsibilities, risks and issues;
    - Reviewing all data protection procedures and related policies annually;
    - Advice and tips to Church Staff and volunteers on how to protect personal data properly;
    - Answering queries from Church Staff and volunteers on ICT and data protection questions;

    - Identifying any contracts or agreements with third parties that might be sensitive in the light of protection of personal information, so that they can be reviewed by the Senior Pastor or eldership before they are signed;
    - Ensuring that all systems, services and equipment used for storing data meet acceptable security standards;
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
- The **Senior Pastor** oversees the Administrative Assistant and is his go-to for any issues related to protection of personal information. Furthermore, the Senior Pastor is responsible for reporting any data leaks to the appropriate Swiss authority and communicating with the individuals affected by a personal data leak.

3. General guidelines

1. The only people able to access personal information should be those who **need it for their work.**
2. Data should **not be shared informally.** When access to confidential information is required, Church Staff can request it from their line managers.
3. **Crossroads** and its people should provide **instruction** to everyone that needs to handle personal information.
4. Church staff and volunteers should **keep data secure** by taking sensible precautions and following the guidelines in this policy.
5. In particular, **strong passwords must be used** and they should **never be shared.** Think about passwords for the Crossroads network, Elvanto, banking software and Quicken accounting software.
6. Personal data **should not be disclosed** to unauthorized people, either within the church or externally.
7. Data should be **regularly reviewed and updated** to make sure it is current. If no longer required, it should be deleted, disposed of or anonymized.
8. People should **request help** from the administrative assistant if they are unsure about any concrete aspect of data protection.

4. Data storage

These rules describe how and where data should be stored safely.

When data is **stored on paper**, it should be kept in a secure place where unauthorized people cannot access it (locked cupboards and filing cabinets). Printouts with personal information should not be left on counters, printers and tables where others can look at them. When the papers with personal information have served their purpose, they should be shredded, not just put in the bin.

When data is **stored electronically,** likewise it should be protected from unauthorized access, accidental deletion and malicious hacking attempts. Think of the following:

- Data should be **protected by strong passwords**, and these passwords should be changed regularly, at least every six months.
- Each person should have their **own passwords** that are not shared with others at all.
- If data is stored on **removable media** like CD, DVD, USB stick, laptop, portable hard drive, these should be kept locked away securely when not being used and not be carelessly handled. Most data security breaches are through careless use of removable media that get lost!

- Data should only be stored on **designated drives and servers** and should only be uploaded to **approved cloud services.**
- Data should be **backed up frequently.** The backup needs to be tested regularly to ensure that it restores properly.
- All servers and computers containing personal information should be protected by **approved and legal security software and firewalls.**
- Personal data should **never be stored on unpaid cloud services** like Dropbox and other services. Remember: if you do not pay for it, the data is the earning model for the supplier.
- **Never transfer personal data over open Internet** links like emails, non-secured Internet sites (http instead of https), and other means which do not supply security.
  Examples: we do not send a list of members in Excel by email; we do not send an Excel or Word list of received donations per donor by email, we do not send passport copies by email, we do not send other forms with personal information (name, address, marital status, passport number, residence permits) by email.

5. Data use

Personal data is of no value to Crossroads, unless it can be used. Therefore, we only collect data that we do something with (minimal data processing). However, when it is used, there is a danger of loss, corruption or theft. Therefore:

- When Church Staff or volunteers work with personal data, we ensure that **screens are locked** when we are away from our screens;
- We **do not share personal data informally** through unsafe methods.
- Personal data must be **encrypted before being transferred electronically.**
- Remote access to servers in the church office should only be done **through safe connections**.
- If personal data is stored outside of Switzerland or the EU, we make sure that it receives the **appropriate data protection in line with Swiss and EU** regulations and cannot be accessed by local governments.
- Church staff should not **save copies of personal data to their own computers.**

6. Data accuracy

The law requires that we take reasonable steps to ensure data is accurate and up to date. This requires Church staff and volunteers who work with personal data to work together on the accuracy. Think of:

- Data will be held in **as few places as necessary**. We should not create unnecessary additional data sets. We use Elvanto, so there is no need to keep separate spreadsheets.
- We take every opportunity to ensure **data is updated.** When we hear about a change affecting someone's information, we ask them to send an email to the office with the updated information.
- Crossroads will make it **easy and safe for members and attenders to update their information**.
- Data should be **updated as mistakes are discovered.** Like: new addresses, spelling mistakes, new phone numbers, etc.

7. The right to know

All individuals who are 'the subject' of personal information that Crossroads records and uses are entitled to:

- Ask **what information** Crossroads holds about them and why
- Ask **how to gain access** to it
- Be informed **how to keep it up to date**
- Ask that wrong information is **rectified**
- Ask that their information be **deleted or anonymized**
- Ask that Crossroads only use the information after **prior approval**
- Be informed how the church is **meeting its data protection obligations**

If someone contacts Crossroads, requesting this information, this is called a 'subject access request'. This should be taken very seriously.

These 'subjects' can exercise their rights by sending an email to: office@crossroadsbasel.ch, expressing the specific information they are requesting, or alternatively they can address their letter to the church's office: Crossroads International Church of Basel, Reinacherstrasse 129, 4053 Basel. Crossroads will provide the information within 14 days of the request, after the identity of the requesting individual has been established.

8. Disclosing data for other reasons

In certain circumstances, applicable Swiss and EU Data Protection Law allows personal data to be disclosed to certain parties (especially law enforcement agencies) without the consent of the individual whose information it concerns.

Under these circumstances, Crossroads will disclose requested information. However, before Crossroads does this, the Senior Pastor will ensure the request is legitimate, seeking assistance from the Elder Board and/or legal advisors where necessary.

Swiss law prevails over EU law, and Swiss and EU law prevail over any other foreign law.

9. Providing information

Crossroads aims to ensure that members and attenders are aware that their information is being processed and that they understand:

- How their information is being used
- How to exercise their rights

To this end, Crossroads has a privacy statement which details how data relating to individuals is used by Crossroads. This statement is attached to this policy and will be published on the Crossroads website.

Privacy Statement

Personal information that Crossroads International Church of Basel gathers is only used for the purpose for which you gave it to Crossroads.

What is personal information?

Personal information is information that can be traced to a specific individual.
Example: the combination of a name and house address, or e-mail addresses including a name and information on donations that Crossroads has received, in combination with a name.

What we will and will not use your information for

Crossroads uses your personal information only for the purpose for which you have given it to Crossroads. We guarantee that your information will never be used for other purposes than giving you the right information about Crossroads and its activities. We will not record any income or wealth information of individual people to use for specific, individually-oriented fundraising for Crossroads. We will never sell your information or make it available to third parties to use for their own purposes.

Consent

We only register your personal information with your express consent, when Crossroads is legally required to do so or where Crossroads has a legitimate interest in recording and using the information. It is assumed that when people give personal information to Crossroads of their own free will, like names, phone numbers and e-mail addresses, in order to receive information from Crossroads, it also entails express consent to register their information for the purpose for which they gave it to Crossroads.

Processing

Crossroads might *add* information to the personal information you gave us, if it is suitable for the proper operation of the church and to know who is doing what. The additional information might, for example, be the 'role' that you undertake in the church at a later stage.
Example: when you start attending the church, we might record your name and e-mail address to send you our weekly updates called 'Crossroads Compass'. Later on, when you become a home group leader, we would add you to a group of home group leaders. When we receive a birth announcement, we will add that you have a son or a daughter.
We use outside parties to manage and/or process your personal information, like a Cloud-based church administrative system and a payroll company. We have agreements in place with these outside parties that they will keep to the same privacy standard as outlined in this Privacy Statement.

Your rights

You have the right to file a complaint if you think we do not keep and process your personal information in the right way. You also have the right to know what we have recorded about you and the right to have this amended if there is information that is not correct. Furthermore, you have the right to request that we will delete or (if legal stipulations prevent that) anonymize your information. We refer you to the Crossroads Data Protection Policy that you may request for from our office.
To contact Crossroads to exercise your rights, send an email to: office@crossroadsbasel.ch or mail us a letter: Crossroads International Church of Basel, Reinacherstrasse 129, 4053 Basel.

Data Storage

By giving us your personal information, you give us permission to record it in our database and to use it for the purpose for which you gave it. As long as your relationship with Crossroads remains active, we will keep your personal information in our database. If we do not see you at Crossroads for an extended period (> 1 year), we will send you an email to ask if you still want to receive Crossroads information or not.
Just to be clear: you do not have to donate financially to Crossroads for us to send you information.

Which information?

Only the personal information that you give to us, or which comes to us in another passive way, will be stored in our database. 'Another passive way' might mean your bank account number and the size of your donations when you donate to Crossroads. All information is treated confidentially. Personal information is only released with your express permission. We do not give your personal information to third parties, unless we are required to do so on legal grounds and only to those parties permitted by Swiss and/or EU legislation.

Location information

If you enter location information on mobile apps or into programs by which you navigate to the church premises, this information will not be stored or used in any other way by Crossroads than the purpose for which you give this information. We cannot guarantee that this will not be done by apps or programs that you are using, as we do not have any influence over that.