POPI Compliance

Table of Contents

Introduction

The passing into law of the Protection of Personal Information Act (POPI) on 1 July 2020 puts the onus on companies and individuals to respect and protect the personal information they process in the course of routine business, including personal information of customers, prospective customers, employees, and suppliers. It is not limited to people but also applies to information about organisations, including communities and corporate entities.

Whilst a lot of work has been put into In Contact to make it compliant, compliance requires involvement from clients as well. This document acts as a framework to identify and assign the different responsibilities.

As a document in draft, I encourage feedback in trying to ensure the safety of the valuable information we are privy to.

Revised: 2022-06-21

Specific Business Purpose or Consent

Overview

POPI requires you to have a particular business purpose for the storage of personal information or explicit consent from the subject. Storing an email address or cell phone number of a recipient who has opted into a newsletter is considered acceptable, but recording someone's religious affinity may not be.

Compliance

In Contact stores the email address and cell phone number of its users. This is used for the different features within the package such as sending test emails and SMSes. This information is not used for any other purpose. In addition cookies are used to record which devices a user has logged in from in order to provide protection from phishing, or stealing of login credentials by a third party.

Each client in turn stores information on the system about their donors, recipients and other contacts. The organization itself needs to be able to prove under review that it has received consent to obtain and store personal data. If authorization is obtained per contact, this can be uploaded and stored against the contact.

Users' access to the organization's data needs to be carefully controlled by limiting their access.

In Contact provides the following means to segregate data:

- A user can be denied access to groups of contacts or allowed access to only one group of contacts.
- Key pairs of data can be controlled by preventing access to address, telephone and email sets of data.
- Pages of related information are defined for an organization. Access to any of the pages can be denied.
- The ability to see donations can be removed.
- The ability to access tax certificates can be removed.
- The ability to access reports can be removed.
- The ability to access the document storage (pictures and document attachments) can be removed.
- A user report should be reviewed regularly to verify access rights.

Maintain the Quality of Your Data

Overview

Personal information must be kept up-to-date and a process must be in place to allow an individual to request and update his or her personal information. If the personal information is no longer being used for a particular business purpose it must be deleted or de-identified so that it cannot be associated back to an individual or company.

If you have a list of contacts that you have stopped communicating to, this must be deleted. If, however, you have an email address or cell phone number of a recipient who has unsubscribed from a list or complained about spam, you can legitimately retain this information to ensure the contact is always filtered out of any communication.

Compliance

In Contact has the feature to send contacts an email with their personal information. Alternatively an email can include a link for them to view or update their details on the website. A copy of any changes is sent to the sender of the email. Consider including a link in each newsletter to access this feature

All bulk emails from the system require an unsubscribe link to be included. Upon unsubscribing the individual will no longer be sent an email but their records will be retained.

One can also add a ‘remove my details’ link in an email to allow a contact to delete themselves from the system, which is suggested for large mailing lists.

Undeliverable emails and SMSes are recorded in the system. These are available in a report and should be corrected on an on-going basis. Details for why an email was undeliverable are recorded against the contact.

Contacts with undeliverable email addresses can be sent an SMS to ask them to update their email address. If responded to, the contact’s email address is automatically updated.

Tools exist within In Contact to manage duplicate records. Duplicate contacts can be identified by a variety of means and their details merged together, in order to maintain the quality of your data.

A list of contacts can be extracted from the system and ordered by the date their data was last updated. This can be used to either update or remove outdated data.

Keep Accurate Records of all Processing

Overview

POPI requires that records be kept of what is done with the personal information. This will include all processing such as when the contact was imported or subscribed, when you sent the contact emails or SMSes, or when they unsubscribed.

Compliance

In Contact logs all changes to contacts. These are available from the diary where they are grouped by date and the user who made the change; on the contact, where they are kept in date order; or from the Activity report, where all changes for a date range can be listed.

After a bulk email is sent, statistics about the email can be accessed from the history tab. This will include details of which emails were undeliverable, delivered and read. By clicking on these links a full list of individuals can be listed.

After a bulk SMS is sent, statistics about the SMS can be accessed from the history tab. This will include details of which SMS were undeliverable and delivered. By clicking on these links a full list of individuals can be listed.

From the contact screen a full list of notes is accessible. These include when the contact was created, updated, email sent, SMS sent, if unsubscribed and if deleted.

Ensure Safety and Security of Data (Users)

Overview

Ensuring the safety and security of data at all times becomes crucial to comply with POPI. Security procedures must be in place for passwords and individuals who have access to any system where the data is stored.

These security measures must extend to all internal processes to ensure compliance when personal information is handled outside of the system. For example, if you email contact lists internally.

Compliance

Device locking is in place for In Contact. When a user logs in, the system checks to see if the user and device combination has previously logged in. If not a verification email is sent to the user, which contains a click that must be clicked. This helps prevent unauthorized access if someone obtains your user name and password.

All user access is controlled by complex passwords. If a password is entered 3 times incorrectly, a Captcha code is displayed on screen, which needs to be entered as well. This helps prevent access against brute hacking.

If a password is entered 10 times incorrectly, In Contact notifies support, who will then investigate further.

Ensure Safety and Security of Data (Website)

Overview

Ensuring the safety and security of a website in order prevent access to data is crucial to comply with POPI. Security procedures must be in place to prevent unauthorized access to any system where the data is stored.

Compliance

Data communications cannot be intercepted:

Communication is managed by Cloudflare. SSL is enabled in full mode using 256 bit encryption: The origin has a valid certificate installed. Using SSL is enforced and augmented with HTTP Strict Transport Security. This policy enforcement protects secure websites from downgrade attacks, SSL stripping, and cookie hijacking. HSTS is an important security mechanism for high security websites.

Geo-locking

Geo-locking is enforced in In Contact. The system is only accessible to countries where its clients are based. This presently excludes the top 10 countries where hacking is known to originate from.

Website Security and Safety:

The hosted server is fully self-managed and behind Afrihost firewalls. Both site and database passwords are complex. The hosting performs backups daily. Further backups are done to Amazon servers daily going back 90 days,

Document Storage:

All uploaded documents for online storage against contact and organizations are offloaded from public access to the website, to being available only through programmatic access. Inadvertent access through search engines and deliberate website crawling is prevented by doing this.

Get Consent to Store Data Offshore

Overview

Many service providers in South Africa store their data in the USA. Under POPI, you are required to get consent to store personal information outside of the borders of South Africa. This can be obtained from your contacts by including a clause in your privacy statement on your website or referring to it when recipients subscribe to your newsletter. You can also refer to it in the footer of your emails to gain consent from existing subscribers.

Compliance

In Contact operates its servers from South Africa.

Disaster Recovery servers and Backup servers are located on Amazon servers. Amazon launched services in South Africa in the first half of 2020 and these services have been relocated to our shores.

The following steps are in place to mitigate any violation of Amazon's very secure servers:

- The Backup servers contain backups going back 90 days for each client. These backups are encrypted and would be unusable if accessed.
- Disaster recovery servers are only loaded for synchronization and then shut down, which is a period of about 10 minutes at a time.
- Each time a Disaster recovery server loads, its IP address changes, making it hard to plan an attack.

Consent must be obtained to Communicate to Prospective Donors

Overview

While best practice email and SMS marketing has always worked this way, the law now compels us to do so. It is now against the law to use direct marketing tactics to sell to a prospective customer without their consent.

You may however contact a recipient once, to obtain this consent (an opt-in campaign) and if they do not explicitly provide you with consent all future communications must cease. Once a recipient opts-in, a method of unsubscribing must be provided as is the current standard practice.

Compliance

In Contact does not provide means to solicit individual's details. It is assumed that when a contact database is taken on, when implementing In Contact, that the donors and supporters are pre-established and existing.

Further contacts added to the system are assumed to have granted consent via the client's website or verbally in their ongoing face to face relationships.

It is not unlikely that a 'subscribe' feature will be added to In Contact in the future. In this event a confirmation mail will be sent when an individual subscribes to a newsletter to prove consent and avoid false subscriptions.

All newsletters from the system require an unsubscribe link to be included. Upon unsubscribing the individual will no longer be sent a newsletter.

The primary email service provider is Amazon. They monitor complaints and state that if the bounce rate exceeds 10% or the complaint rate exceeds 0.1%, they might temporarily block sending of email.

June 2022: As per Amazon the bounce rate across all clients for In Contact is 0.64% and the complaint rate is 0.07%

General Consent versus Specific Consent

Overview

Direct marketing to customers is permitted under POPI without having to get their explicit consent. All other rules still apply though, including being able to only market similar products or services to them.

Compliance

In Contact is not designed to be a direct marketing tool, but the correct way to implement direct marketing is to arrange individuals into groups that identify their various interests and when sending bulk communication, these various groups should be targeted.

As with all bulk email, an unsubscribe link needs to be included. If the individual unsubscribes to a targeted email, they will be removed from the interest that group represents.

For beneficiaries it is best to get their signed consent before adding to the database. A good example of a clause to add is:

“I agree that the above participant’s personal information can be recorded on paper and electronically by XXX. I understand that the above participant’s personal information will not be disclosed to anyone outside of XXX. I agree that the above participant’s information will be used to collect statistics and to help with any necessary communication.”

Transparency of the Sender

Overview

All communications must include the identity and contact details of the sender. Ensure that your company information is a standard part of every email you send. It is also good practice to ensure that your email footer has a complaints link to provide recipients with an option to complain to you if they feel a violation of their privacy has occurred. It is better to receive these complaints and deal with them directly rather than to be reported to the authorities.

Compliance

Ensuring that your mail is well branded is not only good marketing but also removes any doubt in the individual's mind as to who they are receiving the communication from.

It might also be prudent to include an email link to someone in your organization to receive complaints, instead of being reported.

Publishing your own privacy policy might also add to your credibility. A link to it could be included in the footer of your emails.

Buying of Databases

Overview

Purchasing contact information from a third party vendor has never been seen as being ethical, but the law has up until now not restricted it. The POPI act states that a vendor may only pass on information to a third party if they have permission from the recipients to do so. If a marketer receives a database from a vendor (even if they have never sent a message to that database), the vendor may already have infringed POPI and thus you too would be held liable.

Compliance

Do not accept a database from a third party unless you know the vendor has explicit permission from the recipients to pass their personal information on.

Any client found to be buying databases will run the risk of having their services suspended if the reputation of the site is considered threatened.