BIZCOMMUNITY

POPI: Your database butt-kick for 2014

By Kevin Bassett

6 Feb 2014

You've been meaning to do it, last year and the year before ... but in 2014 that untidy customer database may just become a huge liability.

All organisations store personal information about someone - shareholders, employees, customers or suppliers - and all of these are subject to the Protection of Personal Information Act No. 4 of 2013 (POPI), which was signed into law in November.

Businesses: You have 12 months to get your databases and procedures in order! Wise up.

Marketing communications

From a marketing perspective you may not send communications to a person after November 2014 without their deliberate opt-in to receive it. This could mean that every data record in your database will have to be contacted and invited to opt in to receive information or offers from you in 2015.

(That may sound like a long way away, but it isn't. Really. Not in business terms.)

POPI also provides for individuals in a database to ask companies exactly what information they are holding about them, so be prepared to answer a possible flood of queries.

The opportunity

Marketers tend to be information hoarders who frequently have no desire to know how many of their data-records are still valid. Emails and SMSes are dispatched on the basis of 'bigger is better' to hundreds of invalid addresses and mobile numbers. So, you can use the POPI compliance project to completely renovate your database...

Getting started

Getting serious about the security of personal information is easy with a methodical approach:

1. Audit the personal information that you store (both digital and paper-based) to identify what personal information you have, on whom and where. Common examples are names, identity numbers, bank account details, debit or credit card numbers, purchase history and an address.

2. POPI requires that personal information is kept current. When last was it updated? Now is the time to institute procedures to ensure that the correct contact details are always in the database. See this as an opportunity and plan annual, automated, personal information updates.

3. Identify the reasons why you hold that information and whether it is still relevant. Analyse your database and ask whether you absolutely need each data field, remembering that every personal detail carries a risk in the world of identity theft.

For instance, you have an ID number field. Why? Will a date of birth suffice? If so, do you need the day and month? Might it be more appropriate to verify a person's age at a later stage in your business process? And keep it short - the more

information you demand the fewer opt-ins you will receive.

4. Check whether you have deliberate consent from the data subjects. Did they take a physical action to opt in or was it passive, like a pre-checked tick box? Decide whether you should be contacting people on your database to get their conscious opt-in.

5. Assess the current physical and technology safeguards you have in place and decide whether they're adequate to secure the personal information you hold. Pay special attention to high-risk information, like unencrypted digital data found on laptops, tablets, smartphones, and other portable storage devices.

6. Implement and enforce internal policies and procedures to ensure data security.

7. Restrict the access privileges of employees and outside service providers who don't need the information to do their job.

8. Write your Privacy Policy and promote internal private information awareness and start 'POPI training' on privacy and security issues.

The first communication

The professional approach to POPI implementation is to send a communication to every individual on your customer database, covering the following points:

1. Inform them that they are on your database.
2. Explain the benefits of remaining - detail what will be communicated to them.
3. Detail how often they will receive such communications (maximum of ... per month).
4. Tell them if their information will be shared with other companies and if so, which ones and why.
5. Provide them with the details of all personal information you currently hold about them.
• Or, tell them that you are revamping the database and prepare them to receive a simplified customer details form.
6. Publish your Privacy Policy to demonstrate that you take privacy seriously.
7. Ask them to opt in to remain on your database by taking a deliberate physical action.
• You may not pre-check the opt-in box or say that 'No reply' equates to an opt-in. The individual must check a box or reply to the message; in short, take some conscious physical action to say that they opt in.

8. Store proof of this opt-in.

Your response

As customers opt in they should be automatically thanked and welcomed. This is also your best opportunity to ask them to complete your redesigned customer details form. And here's a tip: sweeten the procedure with a reward or voucher for completed forms.

The good news is that all of the above is easily automated using email or SMS and mobile web technology. (SMS is generally considered to have better opening rates than email.)

POPI in a bomb-shell

POPI will bring South Africa in line with international data protection laws by regulating the collection and processing of personal information by public and private organisations. It introduces legal protection for risk of harm arising from the unauthorised collection, processing, misuse or loss of personal information.

Defaulters will be subject to substantial penalties and sanctions, including civil and criminal action. POPI also creates an

enforcement system that is free and accessible to the public.

The Bill requires organisations to establish appropriate policies and procedures to protect the various forms of data that are part of their business operations.

It will have a significant impact on any form of personally directed marketing.

A KISS to close...

Keep it simple:

- Collect the minimum personal information required to achieve your objective.
- Hold it for the shortest time possible.

- Give access to as few people as necessary.

.. and develop a Privacy Policy / Statement that lets individuals know that you take their information security seriously.

ABOUT KEVIN BASSETT

Kevin Bassett, a mobile communications specialist, is the founder and CEO of Floodgate Communications (2004). Floodgate (www.floodgate.co.za) specialises in mobile communication strategies that deliver solutions for marketing and advertising, corporate internal communications, call centres and customer queries. Call Kevin on cell +27 (0)82 652 0530, email kevin@floodgate.co.za, follow @KevBassett and @FloodgateComms on Twitter or SMS kevin to 34007 (R2), and he'll call you right back.

- POPI: Your database butt-kick for 2014 - 6 Feb 2014
- [2013 trends] How to metamorphasise mobile marketing this year - 28 Jan 2013
- Eyeball Time: Buy 30 seconds, engage 3 minutes? - 19 Jul 2012
- [2012 trends] Mobile - why, what and maybe - 16 Jan 2012

View my profile and articles...