Pacific Yearly Meeting Data Breach Policy and Plan

(Working Version)

Published: 6/11/2019 **Approved:** Communications Committee, 6/13/2019

This "Policy and Plan" aims to help PYM manage Personal Data breaches effectively. PYM holds a limited amount of Personal Data about individuals who use services supported by PYM.

PYM places a high premium on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

A data breach generally refers to the unauthorized access to and retrieval of information, which may include corporate and / or Personal Data. Data breaches are generally recognized as one of the more costly security failures of organizations. They could lead to financial losses, and cause Friends to lose trust in PYM.

Scope

This policy applies to all Friends who are responsible for managing data held by PYM. Such Friends must be familiar with this policy and comply with its terms. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be approved by the PYM Communications Committee (PYM ComCom). The committee's Data Breach Team (a subcommittee of ComCom) is charged to fulfill this policy and directly manage any data breach incident responses.

Training

All Friends who manage data held by PYM will receive training on this policy. New members of PYM committees and offices will be offered training within the first month of their new service terms. While some committees and offices such as ComCom, Ministry and Oversight, Youth Programs, Presiding Clerk, Assistant Clerk, and Registrar are likely to manage applicable data, all committees and officers will be offered training on this policy prior to accessing PYM data.

Training will be provided at least once a year and whenever there is a substantial change in the law or our policy and procedure.

Training is provided through one-on-one or small-group review of the policy and applicable laws relating to data protection.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Clerk of PYM ComCom at pym.website@gmail.com.

Personal Data
Personal Data is any information relating to an individual, whether it relates to his or her private, professional or public life. It includes such things as a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address.

Any use of Personal Data is to be strictly controlled in accordance with this policy.

While some data will always relate to an individual, other data may not, on its own, relate to an individual. Such data would not constitute Personal Data unless it is associated with, or made to relate to, a particular individual. Generic information that does not relate to a particular individual may also form part of an individual's Personal Data when combined with Personal Data or other information to enable an individual to be identified.

PYM gathers Personal Data for two purposes: for Annual Session registration and to disseminate contact information among members of the PYM community who need to contact each other. Such Personal Data may include in user profiles:

- Information such as Full name, Mailing address, Email address, and phone numbers
- Information on housing placements and support needs at annual session, such as age, allergies and mobility limitations
- Preferences for participation in aspects of annual session, such as meal preferences, and workshop preferences
- Information to facilitate payment of fees for annual session, such as family members, payment methods, and amounts paid
- User profile information to fulfill insurance or other due diligence requirements, such as results of background checks for adults working with minors in youth programs at annual session or at any other PYM events or activities.

Personal Data that PYM committees gather for internal operational purposes (such as information on job applicants or surveys of participants in PYM-sponsored events) is not stored on the PYM website, but may be stored on devices or online accounts of individual committee members.

Causes of Data Breaches
Data breaches may be caused by Friends responsible for PYM data sets, parties external to the organization, or computer system errors.

Human Error
Human Error causes include:
- Loss of computing devices (portable or otherwise), data storage devices, or paper records containing Personal Data
- Disclosing data to a wrong recipient
- Handling data in an unauthorized way (e.g., downloading a local copy of Personal Data)

- Unauthorized access or disclosure of Personal Data by volunteers or staff (e.g., sharing a login)
- Improper disposal of Personal Data (e.g., hard disk, storage media, or paper documents containing Personal Data sold or discarded before data is properly deleted)

Malicious Activities
Malicious causes include:
- Hacking incidents / Illegal access to databases containing Personal Data
- Theft of computing devices (portable or otherwise), data storage devices, or paper records containing Personal Data
- Scams that trick Friends in PYM into releasing the Personal Data of individuals

Computer System Error
Computer System Error causes include:
- Errors or bugs in applications supporting PYM's website or other software used by PYM or Friends
- Failure of cloud services, cloud computing or cloud storage security / authentication / authorization systems

Reporting Breaches
PYM ComCom has an obligation to report actual or potential data protection compliance failures. This allows us to:
- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify PYM's Ministry and Oversight Committee of data breaches
- Notify law enforcement of any data breach failures that are material either in their own right or as part of a pattern of failures

If a data breach occurs, PYM ComCom will notify any affected individuals without undue delay after becoming aware of a Personal Data breach. However, PYM does not have to notify the data subjects if only anonymized data is breached. That is, the notice to data subjects is not required if the data affected by the data breach has been previously processed to remove any personally identifiable information.

Notifications include the following information, where available:
- Extent of the data breach
- Type and volume of Personal Data involved
- Cause or suspected cause of the breach
- Whether the breach has been rectified
- Information on how individuals affected by the data breach are being notified
- Contact details of PYM ComCom members from whom affected individuals receive further information or clarification

When specific information of a known data breach is not yet available, PYM ComCom will send an interim notification, comprising a brief description of the incident.

Data Breach Team

The Data Breach Team (DBT) is a subcommittee of PYM ComCom and shall include the Clerk of PYM ComCom.

Data Breach Management Overview

Upon being notified of a (suspected or confirmed) data breach, the Data Breach Team will immediately initiate the data breach management & response plan.

PYM ComCom's data breach management and response plan is:

1. Confirm the Breach
2. Contain the Breach
3. Assess Risks and Impact
4. Report the Incident
5. Evaluate the Response & Recovery to Prevent Future Breaches

Confirm the Breach
The DBT will act as soon as it is aware of a data breach. When possible, it should first confirm that the data breach has occurred. It may make sense for the DBT to proceed to contain the breach on the basis of an unconfirmed reported data breach, depending on the likelihood of the severity of risk.

Contain the Breach
The DBT should consider the following measures to contain the breach, where applicable:

- Shut down the compromised system that led to the data breach.
- Establish whether steps can be taken to recover lost data and limit any damage caused by the breach. (e.g., remotely disabling / wiping a lost notebook containing Personal Data of individuals.)
- Prevent further unauthorized access to the system.
- Reset passwords if accounts and / or passwords have been compromised.
- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and/or remove external connections to the system.

Assess Risks and Impact
Knowing the risks and impact of data breaches will help PYM ComCom determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

Risk and Impact on Individuals

- How many people were affected?

A higher number may not mean a higher risk, but assessing this helps overall risk assessment.

- Whose Personal Data had been breached?
  Does the Personal Data belong to committee members, website visitors, or minors? Different people will face varying levels of risk as a result of a loss of Personal Data.
- What types of Personal Data were involved?
  This will help to ascertain if there are risks to reputation, identity theft, safety and/or financial loss of affected individuals.
- Any additional measures in place to minimize the impact of a data breach?
  Eg., a lost device protected by a strong password or encryption could reduce the impact of a data breach.

Risk and Impact on organizations

- What caused the data breach?
- Determining how the breach occurred (through theft, accident, unauthorized access, etc.) will help identify immediate steps to take to contain the breach and restore public confidence in the management of Personal Data by PYM.
- When and how often did the breach occur?
  Examining this will help PYM ComCom better understand the nature of the breach (e.g., malicious or accidental).
- Who might gain access to the compromised Personal Data?
  This will ascertain how the compromised data could be used. In particular, affected individuals must be notified if Personal Data is acquired by an unauthorized person.
- Will compromised data affect transactions with any other third parties?
  Determining this will help identify if other organizations need to be notified.

Report the Incident

By notifying affected individuals if their Personal Data has been breached, PYM ComCom will encourage individuals to take preventive measures to reduce the impact of the data breach, which will also help rebuild community trust in PYM and PYM ComCom.

Whom to Notify:

- Notify individuals whose Personal Data has been compromised.
- Notify other third parties such as banks, credit card companies or law enforcement, where relevant.
- Law enforcement should be notified if criminal activity is suspected (e.g., hacking, theft or unauthorized system access by an employee).

When to Notify:

- Notify affected individuals immediately if a data breach involves sensitive Personal Data so they may take the necessary actions early to avoid potential abuse of the compromised data.
- Notify affected individuals when the data breach is resolved or if any material new information is learned.

Notification overview:

- The Data Breach Team will reach out via email and telephone to affected individuals, taking into consideration the urgency of the situation and number of individuals affected.
- Notifications will be specific, in plain language and provide clear instructions on what individuals can do to protect themselves, including:
    - How and when the data breach occurred, and the types of Personal Data involved in the data breach.
    - What PYM ComCom has done or will be doing in response to the risks brought about by the data breach.
    - Specific facts on the data breach, where applicable, and actions individuals can take to prevent that data from being misused or abused.
    - Contact details and how affected individuals can reach members of the DBT and PYM ComCom for further information or assistance (e.g., phone numbers, e-mail addresses, webpage links).

Evaluate the Response and Recovery to Prevent Further Breaches

After steps have been taken to resolve the data breach, PYM ComCom will review the cause(s) of the breach and evaluate whether existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring again. Wherever possible, PYM ComCom will put a stop to practices that led to the data breach. This will encompass operational and policy-related issues, resource concerns and issues concerning the internal procedures of PYM ComCom.

A brief report on any data breach incident and the corrective actions taken by PYM ComCom will be posted on our website. A full post-incident analysis will be made available to anyone who requests it.

Monitoring

- All Pacific Yearly Meeting committee and staff members and volunteers with access to PII data on PYM members must observe this policy.
- PYM ComCom has overall responsibility for this policy.
- PYM ComCom will review and monitor this policy in response to changes in technology, regulatory or legal changes or new concerns or data breach incidents.