DATA BREACH RESPONSE PLAN

DEFINITIONS

'Eligible breach': A data breach requiring mandatory notification to the Office of the Australian Information Commissioner (OAIC)

'Staff member': In this plan, references to "staff member" apply to employed National Office staff and volunteers appointed to Multiple District Committees.

'Data breach response plan': This plan and accompanying checklist.

1) This Data Breach Response Plan (Response Plan) sets out the procedure to be followed by the staff of MD201 of Lions Clubs International (Lions Australia)Lions Australia experiences a data breach, or suspects that a data breach has occurred.
2) A data breach occurs when personal information (defined in section 6 of the Privacy Act 1988 (Cth)) is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Personal information refers to information that identifies or reasonably identifies an individual.
3) Adherence with the Response Plan will ensure Lions Australia can contain, assess and respond to data breaches in a timely fashion in order to mitigate potential harm to affected persons.
4) This plan:
   a) sets out the roles and responsibilities of staff and volunteers;
   b) sets out the contact details of appropriate staff in the event of a data breach; and
   c) outlines the procedure to be followed in the event of a data breach.
   d) outlines particular measures for the mandatory notification of 'eligible breaches'.

Staff member to notify Executive Officer

5) Immediately notify the Executive Officer of the suspected data breach.
6) Record and advise the Executive Officer of the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and the context of the affected information and the breach.

Executive Officer to make an initial assessment of the breach

7) The Executive Officer must initially assess and determine whether a data breach has occurred and the suspected degree.
8) Minor breaches will be logged on the attached checklist.
9) "Eligible data breaches" require notification to the Office of the Australian Information Commissioner(OAIC)
10) According to the OAIC, an 'eligible data breach' that is, one that requires notification to the OAIC, occurs when the following three criteria are satisfied:[1]
    a) there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds,
    b) this is likely to result in serious harm to one or more individuals, and
    c) the entity has not been able to prevent the likely risk of serious harm with remedial action.

[1] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches

Assessing a Breach

11) If there is any suspicion that an 'eligible breach' has occurred, the Executive Officer must immediately notify the Council Chairperson and Legal Officer.
12) Investigation of breaches must be carried out within 30 days of notification.
13) A minor breach should be dealt with by the Executive Officer who is also the Privacy Officer. Details will be logged on the checklist.
14) If the breach is serious, it must be escalated to the Multiple District Executive.

Breach Assessment and resolution process

15) There are four key steps to consider when responding to a breach or suspected breach. Generally, steps 1-3 should be carried out concurrently or in close succession.
16) Investigation and resolution of any data breach must be documented on the attached checklist. Assessment of breaches is largely subjective, however will be reported as follows:
    a) Minor breaches will be logged on the checklist and archived.
    b) Serious breaches will be logged on the checklist, archived and reported to the Executive.
    c) Eligible breashes will be logged on the checklist, reported to the OICD as indicated in this procedure, reported to Council and archived.

Procedure

17) Step 1: Contain the breach and make a preliminary assessment
    a) Once a data breach has been identified, action must be taken to immediately contain it. For example, stop the unauthorised practice, recover the records or shut down the system that was breached.
18) Initiate a preliminary assessment - The following questions should be addressed when making the preliminary assessment:
        i) What information does the breach involve?
        ii) What was the cause of the breach?
        iii) What is the extent of the breach?
        iv) What are the harms (to affected persons) that could potentially be caused by the breach?
        v) How can the breach be contained?
    b) Step 2: Evaluate the risks associated with the breach - The following factors are relevant when assessing the risk:
        i) The type of information involved?
            (1) Is it personal information?
            (2) Does the type of information hold a greater risk of harm?
            (3) Who is affected by the breach?
        ii) Determine the context of the affected information and the breach
            (1) What is the context of the information involved?
            (2) What parties have gained unauthorised access to the affected information?
            (3) How could the information be used?
        iii) Establish the cause and extent of the breach
            (1) Is there a risk of ongoing breaches or further exposure of the information?
            (2) Is there evidence of theft?
            (3) Is the information adequately encrypted, anonymised or otherwise not accessible?
            (4) What was the source of the breach? (risk of harm may be lower where source of the breach is accidental rather than intentional)

(5) Has the information been recovered?
(6) What steps have already been taken to mitigate the harm?
(7) Is this a systemic problem or an isolated incident?
(8) How many persons are affected by the breach?

iv) Assess the risk of harm to the affected persons
(1) Who is the recipient of the information?
(2) What harm to persons could result from the breach?

v) Assess the risk of other harms
(1) Other possible harms, including to the agency or organisation that suffered the breach. For example:
(a) Reputational damage
(b) Legal liability

19) Step 3: Notification

a) In general, if a data breach creates a real risk of serious harm to a person, the affected person should be notified.
b) The key consideration is whether notification is necessary to avoid or mitigate serious harm to an affected person.
c) Consider the following factors:
i) What is the risk of serious harm to the person as determined by step 2?
ii) What is the ability of the person to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the agency or organisation)?
iii) Even if the person would not be able to take steps to fix the situation, is the information that has been compromised sensitive or likely to cause humiliation or embarrassment?
iv) What are the legal and contractual obligations to notify and what are the consequences of notification?

20) Notification process - In general, notification should occur as soon as reasonably possible. However, in some instances, delay may be necessary.
21) Notification should be direct – by phone, letter, email or in person, to the affected individuals.
22) Indirect notification, either by website, posted notices or media should only occur where direct notification could cause further harm, is cost prohibitive or the contact information for affected persons is unknown.
23) Details to include in the notification
a) The content of the notification will vary depending on the particular breach and notification method. However, the OAIC recommend that notifications should include the following information:
i) incident description;
ii) type of information involved;
iii) response to the breach;
iv) assistance offered to affected persons;
v) other information sources designed to assist in protecting against identity theft or interferences with privacy (e.g. www.oaic.gov.au);
vi) Lions Australia contact details;
vii) whether breach notified to regulator or other external contact(s);
viii) legal implications;
ix) how individuals can lodge a complaint; and
x) how individuals can lodge a complaint with the OAIC (where the information is personal information).

Executive review

24) Serious breaches will be reported the Executive for notation and review, if necessary.
25) Eligible Breaches must be escalated to the Executive within 24 hours of the breach having been identified.
26) Once a matter has been escalated to the Multiple District Executive the investigation and management of the breach is managed according to the checklist.
27) Where the breach is assessed as meeting the criteria for an 'eligible breach, the Executive Officer will complete the formal notification of the breach to the OAIC, using the online form.

    https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB
28) An eligible breach, the matter must be reported to the next available meeting of the Multiple District Council, including recommendations:
    a) to make appropriate changes to policies and procedures if necessary;
    b) revise staff training practices if necessary; and
    c) update this Response Plan if necessary.
29) There may also be appropriate to notify other third parties, such as:
    a) The Police.
    b) Insurance providers.
    c) Credit card companies, financial institutions.
    d) Professional or other regulatory bodies.
    e) Other internal or external parties who have not already been notified.
    f) Agencies that have a direct relationship with the information lost/stolen.
30) Step 4: Prevent future breaches:
    Once immediate steps have been taken to mitigate the risks associated with a breach, Lions Australia must take the time to investigate the cause of the breach.