Heffron

Privacy Breach Notification Protocol

January 2020

CONTENTS

Introduction

The purpose of this procedure is to provide all stakeholders guidance on how to manage all privacy breaches reported within Heffron to closure and reporting to the OAIC if required.

Heffron has prepared this protocol to ensure that it:

a) complies with the introduction of the new Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) and other applicable privacy laws and obligations; and
b) works together to minimise the impact of and protect against data breaches.

Who must read this protocol

If you supply, access or otherwise deal with information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) whether the information or opinion is true or not; and
b) whether the information or opinion is recorded in a material form or not,

through or for Heffron (Heffron Personal Information), then this protocol applies to you.

Eligible breach

For the purpose of this protocol, an Eligible Data Breach occurs where:

a) There has been either unauthorised access to, unauthorised disclosure of or a loss of personal information that is likely to result in serious harm to one or more individuals;
b) a reasonable person would conclude these circumstances are likely to result in serious harm to an individual who has Personal Information relating to them at risk from the unauthorised access / disclosure (Affected Individual); and
c) Heffron has not been able to prevent the likely risk of serious harm with remedial action.

Your obligations

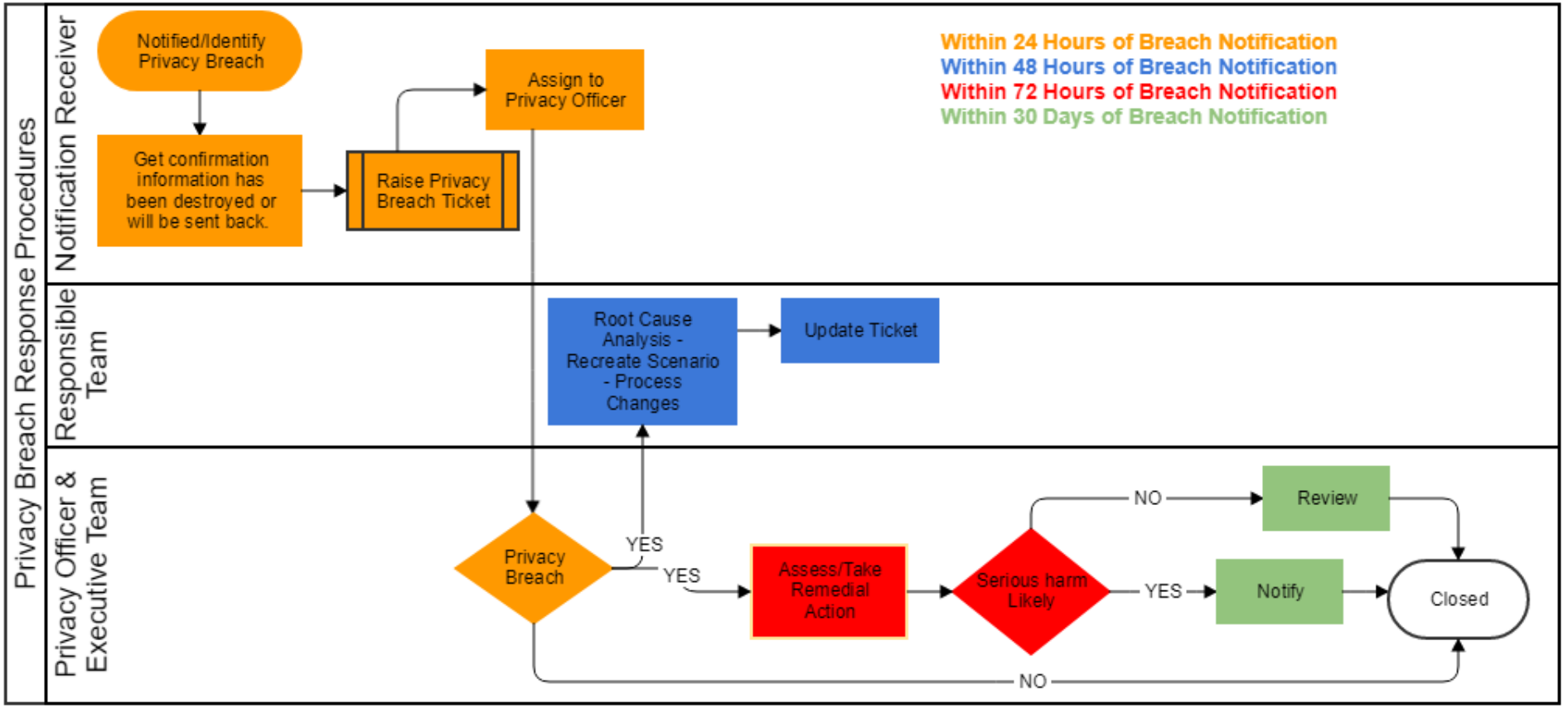
You must:

a) immediately notify us if you become aware of (or suspect that there has been) any unauthorised access to, disclosure or loss of, or any other unauthorised interference with, any Heffron Personal Information; and
b) comply with the procedure set out on page 5 of this protocol.

Related Policies

Please refer to the Privacy Policy for additional information.

Process workflow



Procedure work instructions

Step	Process Description	Responsible Party	Procedure Steps	Related Procedure
1	Breach Information	Breach Notification Receiver	**Discuss with breach notifier:** 1. Explain importance of destroying the information or providing it back to us. 2. Offer to have a courier come to collect, send a prepaid envelope or have them return to sender. 3. Escalate to Head of Customer, CRM or any other executive if required.	
2	Raise Privacy Breach Jira Ticket	Breach Notification Receiver	**Obtain and record in ticket:** 1. Date breach was received. 2. Description of the breach. 3. If confirmation that the information was destroyed was received. 4. If the Breach Notifier intends to send the information back. 5. Any contact details obtained not already on file.	
3	Assign ticket to Privacy officer	Breach Notification Receiver	Assign ticket to Privacy Officer	
4	Privacy Officer	Breach Assessment	Review the Jira Ticket, discuss with the responsible team and determine if this is indeed a Privacy Breach.	

Step	Process Description	Responsible Party	Procedure Steps	Related Procedure
5	Root Cause Analysis	Responsible Team Lead	Workshop with the team what the root cause of the privacy breach was, recreate the issue and identify all processes improvements that can be made to ensure it never happens again. Coordinate involving any other teams, executive as required.	
6	Assess/Take Remedial Action	Core Executive Team	As a group follow the OAIC Privacy Breach Response Procedures and determine the Likelihood of Serious Harm and if the Privacy Breach Needs to be notified to OAIC.	OAIC Privacy Breach Response Procedures.pdf
7	Review	Core Executive Team	As a group follow the OAIC Privacy Breach Response Procedures and review the Privacy Breach to ensure that all mitigants have been put into place.	OAIC Privacy Breach Response Procedures.pdf
8	Notify	Core Executive Team	As a group follow the OAIC Privacy Breach Response Procedures and prepare the Part 1 and Part 2 of the Notifiable Response Report, notify the OAIC and the affect parties.	OAIC Privacy Breach Response Procedures.pdf

Potential breaches and remedial actions

Potential breaches

The following is a list of potential eligible data breaches. This list is for example only and is no way intended to be an exhaustive list. If you are unsure of what constitutes a breach, please escalate to Head of Customer, CRM or any other executive.

a) Heffron terminates an employee with access to Heffron Personal Information but does not remove the employee's authorised access in a timely manner.
b) A data file, laptop, smartphone, or other device containing Heffron Personal Information is sent to the wrong recipient or is otherwise lost.
c) An application vulnerability on a Heffron website, server or system allows access to Heffron Personal Information.
d) Laptops, devices, software or applications used by Heffron employees in systems that have access to Heffron Personal Information are critically out-of-date or are unencrypted.
e) A Heffron employee leaves hard copies of documents containing Heffron Personal Information in a customer or service provider meeting room, and that customer or service provider would not otherwise have access to that Heffron Personal Information.

Potential remedial actions

a) Implement a policy ensuring that authorised accesses are revoked immediately when employees are terminated or otherwise leave. Reasonably refresh passwords and other security around the Heffron Personal Information from time to time.
b) Immediately reach out to the recipient to notify them that they should not access the Heffron Personal Information and return or delete it or ask the relevant IT support staff to remotely wipe the Heffron Personal Information form the device where possible.
c) Run periodic checks for application vulnerabilities and security system reviews.
d) Ensure devices and software are auto-updated, and relevant devices are encrypted.
e) Immediately reach out to the customer or service provider that they must not read the documents and must store the documents in a safe place until Heffron can retrieve them.