Data Breach Notification Protocol

Date of Protocol: 22/02/2018

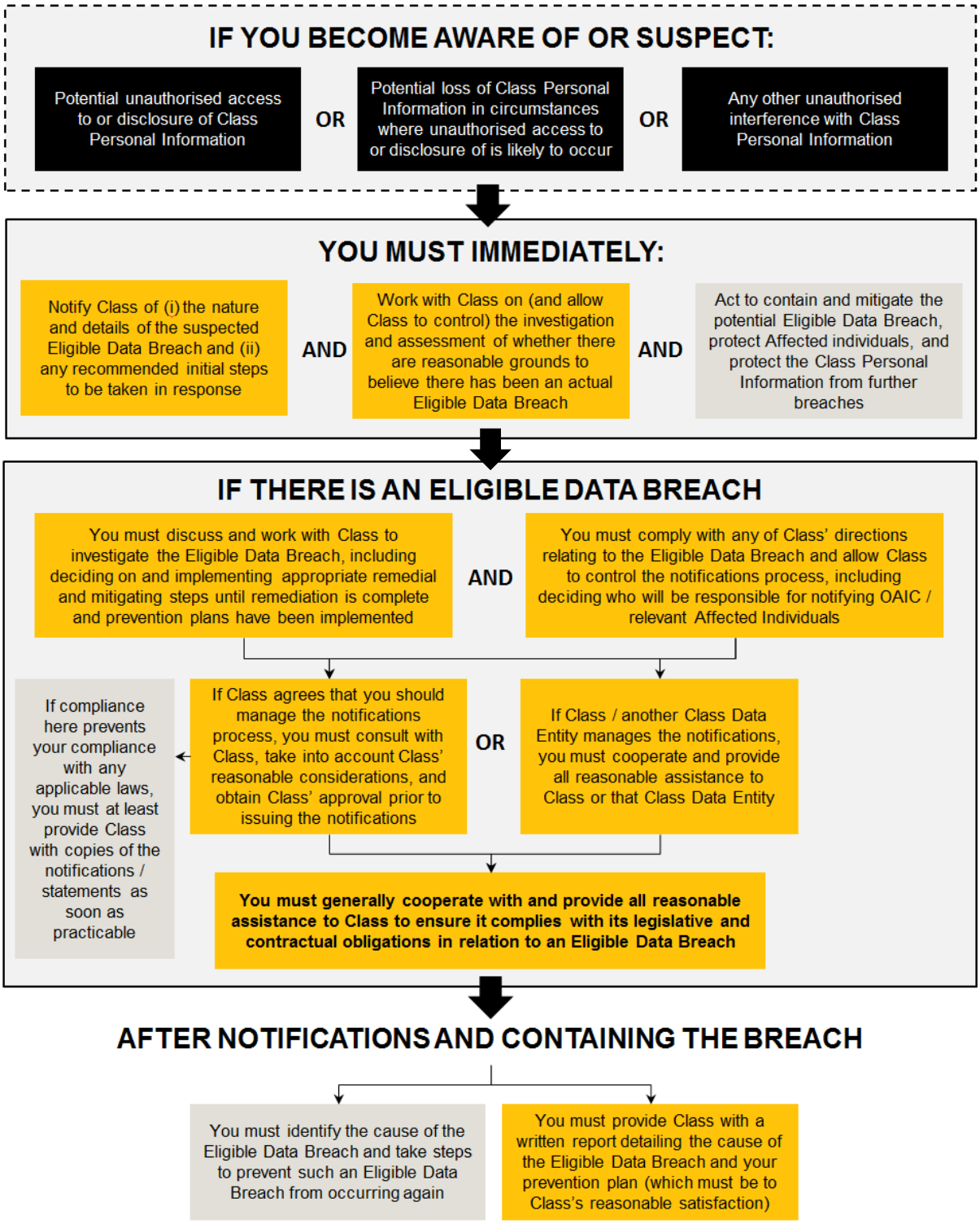
Version: 1.0

Class Super Pty Ltd

I. OVERVIEW

1. 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 Class (**Class Personal Information**), then this protocol applies to you and you are a **Class Data Entity**.
2. WHY THIS PROTOCOL IS IMPORTANT	Class has prepared this protocol to ensure that it and all Class Data Entities: (a) comply with the introduction of the new *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) and other applicable privacy laws and obligations; and (b) work together to minimise the impact of, and protect against data breaches.
3. ELIGIBLE DATA BREACHES	For the purpose of this protocol, an **Eligible Data Breach** occurs where: (a) there has been either unauthorised access to / disclosure of Class Personal Information, or Class Personal Information has been lost in circumstances where there will likely be unauthorised access / disclosure; (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) remedial steps cannot be taken to either prevent the unauthorised access / disclosure before it happens or prevent the serious harm to the Affected Individuals before it occurs.
4. YOUR OBLIGATIONS	You must: (a) **notify**: immediately notify Class 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 Class Personal Information; (b) **process**: comply with the process set out on page 2 of this protocol; and (c) **audit**: allow Class to undertake reasonable periodic reviews to test and validate your compliance with this protocol.
5. FURTHER RESOURCES	The Office of Australian Information Commissioner (**OAIC**): www.oaic.gov.au *Privacy Act 1988* (Cth): https://www.legislation.gov.au/Details/C2017C00283

II. DATA BREACH NOTIFICATION PROCESS



III. EXAMPLES

1. POTENTIAL ELIGIBLE DATA BREACHES	(a)	A Class Data Entity fires an employee with access to Class Personal Information, but does not remove the employee's authorised access to, or change applicable passwords or other security around the Class Personal Information in a timely manner.
	(b)	A data file, laptop, smartphone, or other device containing Class Personal Information is sent to the wrong recipient or is otherwise lost.
	(c)	An application vulnerability on a Class Data Entity website, server or system allows access to Class Personal Information.
	(d)	Laptops, devices, software or applications used by Class Data Entities in systems that have access to Class Personal Information are critically out-of-date or are unencrypted.
	(e)	A Class Data Entity employee leaves hard copies of documents containing Class Personal Information in a customer or service provider meeting room, and that customer or service provider would not otherwise have access to that Class Personal Information.
2. POTENTIAL REMEDIAL OR PROTECTIVE 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 Class Personal Information from time to time.
	(b)	Immediately reach out to the recipient to notify them that they should not access the Class Personal Information and return or delete it, or ask the relevant IT support staff to remotely wipe the Class 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 the Class Data Entity employee can retrieve them.