FOI 119-2023

Data Breach Response Plan

Nous Group

10 December 2021

nous

Contents

1 Introduction 1
2 Identification 1
2.1 Detecting a data breach 1
2.1.1 Privacy Information 1
2.1.2 Government Classified Information 2
2.1.3 Client Sensitive Information 2
3 Triage – determining if the breach is 'notifiable' 2
3.1.1 Australian Privacy Information 2
3.1.2 UK Privacy Information 2
3.1.3 Canadian Privacy Information 3
3.1.4 Government classified 3
3.1.5 Client Sensitive Information 3
4 Escalation 3
5 Data Breach Response 4
5.2 Incident Response Team 5
5.3 Containment 5
5.4 Assessment of 'serious / significant' harm 6
5.5 Reporting and Notification 6
5.5.1 Australian Privacy Information 6
5.5.2 UK Privacy Information 7
5.5.3 Canadian Privacy Information 7
5.5.4 Privacy Information breach – other jurisdictions 7
5.5.5 Government Classified Information 7
5.5.6 Client Sensitive Information 7
5.6 Communicating to affected individuals 8
5.7 Review 8
5.8 Post-breach actions 8
6 Training, testing and review 8

1 Introduction

Nous Group ('Nous') is proud of being a purpose-driven organisation where clients are our first priority. By adopting a risk-based approach, Nous has implemented various safeguards to protect privacy information, government classified information and client sensitive information (collectively 'high-risk / sensitive information').

A data breach occurs when any high risk / sensitive information that is held by Nous is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference.

In the unlikely and unfortunate event of a data breach, it is critical that we move quickly to identify and contain the incident and notify any relevant parties. This **Data Breach Response Plan** ('Plan') is designed to guide Nous to act quickly by defining the roles and responsibilities of the Data Breach Response Team and outlining the steps they should follow to effectively manage the breach.

This Plan also aims to assist Nous to:

- meet legislative and contractual obligations in relation to mandatory data breach notification requirements
- protect our client's and Nous' reputation
- respond to adverse media or stakeholder attention from a breach or suspected breach
- instil confidence in Nous' capacity to protect sensitive information by properly responding to a breach.
- review lessons learnt and to improve our data breach response processes

2 Identification

2.1 Detecting a data breach

A data breach could occur because of a system breach, a process failure, malicious action or inadvertent behaviour, which could potentially result in harm to an individual or client and expose Nous to reputational damage as well as legal and financial penalties

Nous employees are required to speak up whenever they see or suspect a data breach has or may have occurred by contacting security@nousgroup.com. After a breach is discovered, Nous must act as soon as possible to minimise the impact on our client organisation(s) and/or the affected individuals.

The following describes the various types of high-risk / sensitive information that may be involved in data breach.

2.1.1 Privacy Information

This includes information about an Individual, which is reasonably, directly, or indirectly identifiable i.e., information which, on its own, or combined with other data, could identify an individual.

Privacy Information is also known as **Personal Information (PI), Personal and Sensitive Information, Personal Data** and **Personally Identifiable Information (PII)** depending on the jurisdiction of each country. The links below provide further guidance for the countries where Nous currently operates:

- Australia: https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information
- UK: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

- Canada: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-1

2.1.2 Government Classified Information

At Nous, 'Government Classified Information' means Australian, UK or Canadian government information which has a security classification applied, depending on its sensitivity.

The document owner (usually the government agency) is responsible for applying the classification – not Nous. The level of classification determines what physical and technical security measures need to be applied to protect that information depending on the government defence agency of each country. The links below provide further guidance for the countries where Nous currently operates:

- Australia: https://www.protectivesecurity.gov.au/publications-library/policy-8-sensitive-and-classified-information
- UK: https://www.gov.uk/government/publications/government-security-classifications
- Canada: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32614

2.1.3 Client Sensitive Information

'Client Sensitive Information' includes commercially sensitive information (e.g., financial records or situation, monetary dealings and mergers and acquisitions, strategic or marketing plans, suppliers and customers, or intellectual property), anything else the client has requested Nous to keep confidential or anything which could cause reputational damage or loss of competitive advantage for that client.

3 Triage – determining if the breach is 'notifiable'

The s 47(1)(b) [redacted] and the s 47(1)(b) [redacted]) will assess the severity and potential impact of the incident and:

- validate whether a data breach has occurred
- use the following information as a guide to determine whether a 'notifiable' data breach has occurred
- seek advice from Nous' Legal team

3.1.1 Australian Privacy Information

In Australia a notifiable data breach is referred to an 'eligible data breach', and must meet the following criteria:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that Nous holds
- this is likely to result in serious harm to one or more individuals and
- Nous has not been able to prevent the likely risk of serious harm with remedial action

3.1.2 UK Privacy Information

In the UK, a notifiable data breach is referred to as a 'personal data breach' and includes the following:

- a security incident that has affected the confidentiality, integrity or availability of personal data

- if not addressed in an appropriate and timely manner, the data breach could result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned
- if the data breach means that a risk to people's rights and freedoms are likely, the breach must be reported to the UK Information Commissioner's Office (ICO)

3.1.3 Canadian Privacy Information

In Canada, a notifiable data breach is referred to as a 'breach of security safeguards' and is defined as the loss of, unauthorized access to or unauthorized disclosure of personal information that pose a real risk of significant harm to individuals.

3.1.4 Government classified

Any unauthorised access and/or disclosure of government information must be triaged by the HISR and the Security Officers of each respective country to determine whether it is a notifiable data breach.

3.1.5 Client Sensitive Information

A notifiable breach would be a disclosure of client sensitive information which is likely to result in:

- significant reputational, legal, financial or other harm to a client
- significant reputational, legal, or financial or other risk to Nous
- a breach of contractual obligations

4 Escalation

Depending on the type of information involved in the data breach, the [redacted] and [redacted] will form the Incident Response Team with the appropriate employees, such as [redacted] the [redacted], [redacted], People team, a subject matter expert and/or other key employees, depending on the nature of the incident, the type of information breached and the country that the incident occurred in.

The Incident Response Team will then follow the steps outlined in the Nous Information Security Incident Response Plan (internal document), i.e., investigate, contain, eradicate, respond, report and conduct root cause analysis.

5 Data Breach Response

The following flowchart outlines Nous' response to a data breach.

5.1.1.1 DATA BREACH RESPONSE PROCESS

s 47(1)(b)

[redacted]

5.2 Incident Response Team

The Incident Response Team will be made up of the following Nous employees, depending on the type of information breached and the country the breach occurred in.

The key responsibilities of each role in relation to managing a data breach are outlined in the table below. More detailed responsibilities of these roles during incident response activities are outlined in Nous' Information Security Incident Response Plan (internal document).

Role	Responsibilities

s 47(1)(b)

[redacted]

5.3 Containment

The Incident Response Team will focus on containment activities to prevent the breach from worsening and to preserve evidence. This may include isolating affected IT systems and/or preventing access to those systems from other employees.

The Incident Response Team will investigate how the breach occurred and retain copies of evidence gathered, which may include interview notes, screen shots, photos or files.

From this evidence, the Incident Response Team will investigate and analyse the root cause of the breach, any internal or external parties who may have been involved, and vulnerabilities or failed safeguards that contributed to the breach.

At each of the data breach response stages, the [redacted] will ensure records the activities are kept, to form the basis of internal incident and post-activity reports, as well as any notifications if required.

5.4 Assessment of 'serious / significant' harm

The Incident Response Team (including the Legal team) will assess whether the data breach has or has the potential to result in serious / significant harm to a client and/or an individual. When this is unclear, the Incident Response Team will seek guidance from the affected client(s) and/or an external legal advisor.

For privacy information breaches, here are some links from each country's regulator's websites for guidance:

Australia: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme#is-serious-harm-likely

UK: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatbreachesdo

Canada: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_6

https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_1

If the Incident Response Team determines that the data breach does not have a risk of causing serious harm, Nous is still required to document the incident and the reasons and justification for this decision.

5.5 Reporting and Notification

Depending on the nature of the data breach and assessment of serious harm, Nous may be required to report the breach to several different stakeholders, including regulatory bodies, law enforcement, individuals or organisations affected by the data breach.

In some circumstances, Nous' clients, subcontractors or vendors may be involved in or contributed to the data breach. If a single eligible data breach applies to multiple entities, only one entity needs to notify the respective commissioner(s) and individuals at risk of serious harm.

Some contracts include clauses around who is responsible for reporting a data breach if one were to occur, so the contract(s) of any affected clients must always be checked before proceeding with the notification. In other cases, the entity (i.e., client, subcontractor or vendor) who was primarily responsible for the data breach and/or has the most direct relationship with the affected individual(s) will be responsible for notifying the affected individuals and/or respective regulator.

Where it is not possible to notify affected individuals, Nous will publish the notification on its website.

The following outlines when notification is required, depending on the type of information involved in the breach and the country where the data breach occurs.

5.5.1 Australian Privacy Information

According to Australian privacy legislation, **within 30 days of becoming aware of the data breach**, Nous must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe it is an eligible data breach (i.e., an unauthorised disclosure or loss of personal information which is likely to result in serious harm to the affected individuals).

As soon as practicable after becoming aware of the data breach, Nous must prepare a statement to the OAIC in accordance with the Privacy Act 1988 (Cth) Sec26WK and notify the affected individuals with the contents of that statement.

Note: failing to comply with the Australian Privacy Act could result in fines, (the value is determined depending on whether health records are involved and/or the seriousness of the privacy breach).

5.5.2 UK Privacy Information

According to UK privacy legislation, if the data breach is likely to result in a risk of the affected individual(s) rights and freedoms, Nous must notify the Information Commissioner's Office (ICO) without undue delay, but no later than **72 hours** of becoming aware of the breach. If the full details are not available within 72 hours, Nous must explain the delay to the ICO and when Nous expect to submit more information.

Nous must also notify affected individuals whose rights and freedoms are at risk without undue delay.

Note; failing to notify the ICO of a breach when required to do so can result in a fine of up to £8.7 million or 2 per cent of Nous' global turnover.

5.5.3 Canadian Privacy Information

According to Canadian Privacy Information, Nous is required to submit a PIPEDA breach report form to the Commissioner and a notification to affected individual(s) for a breach of security safeguards involving personal information under Nous' control if it is reasonable to believe there is a real risk of significant harm (RROSH) to an individual.

When Nous has considered that the breach poses a real risk of significant harm, Nous must notify the affected individuals and the Privacy Commissioner **as soon as feasible**. After submitting the report, Nous has the ability of submitting any new information about the breach once becoming aware of it.

It is an offence to knowingly contravene PIPEDA reporting, notification and record-keeping requirements, and doing so could lead to fines.

Where a significant cyber incident occurs, Nous may also need to report this to the National Cyber Security Centre (the NCSC).

5.5.4 Privacy Information breach – other jurisdictions

For breaches involving other jurisdictions, Nous s 47(1)(b) and the s 47(1)(b) will assess whether Nous also needs to notify other international regulators. Where it is not clear, guidance will be sought from an external legal provider.

5.5.5 Government Classified Information

For data breaches involving Australia Government Information, the Security Officer will submit an incident report according to the DISP requirements within 24 hours of the discovery of the security incident.

For data breaches involving UK Government information, the following link provides guidance on how to report a data breach: https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/signalement-reporting-eng.html#s6. The breach must be reported within 24 hours.

For data breaches involving Canadian government information, the following link provides guidance on how to report a data breach. https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/signalement-reporting-eng.html#s6. The report must be submitted "as soon as possible".

5.5.6 Client Sensitive Information

In the event of a client sensitive information breach, where serious harm from the breach cannot be mitigated through remedial action and/or we are required to notify the client due to contractual obligations, Nous will notify the relevant client organisation(s) as soon as practicable.

In Australia, where required, and in consultation with the affected client, a report may also be made to the Australian Cyber Security Centre (https://www.cyber.gov.au/report).

5.6 Communicating to affected individuals

Some contracts include clauses around who is responsible for communicating with affected individuals if a data breach were to occur, so the contract(s) of any affected clients must always be checked before proceeding with a communication plan. In other cases, the entity (i.e., client, subcontractor or vendor) who was primarily responsible for the data breach and/or has the most direct relationship with the affected individual(s) will be responsible for communicating the data breach with the affected individuals.

In the event that Nous is responsible for communicating the data breach with the affected individuals, and depending on the nature of the breach, the s 47(1)(b) and s 47(1)(b) will work with the s 47(1)(b) and/or the relevant Client Manager to implement an appropriate communications strategy which could include:

- notifying all individuals
- notifying only those individuals at risk of serious / significant harm
- publishing a statement on Nous' website and publicising it

Written notification will be from the s 47(1)(b) and Nous will use a reasonable method to notify individuals, such as email, physical mail or telephone call. The s 47(1)(b) must be confident that the method used will ensure individuals become aware of the breach and understand the notification.

Following notification, the s 47(1)(b) and s 47(1)(b) will determine the information to be reported to Nous' Executive Board and s 47(1)(b), including the timing of notifications.

5.7 Review

The s 47(1)(b) will record the details of each data breach (including those not escalated to the Incident Response Team). Following resolution of each breach, the s 47(1)(b) will conduct a post-breach review to assess Nous' response and the effectiveness of the Data Breach Response Plan.

5.8 Post-breach actions

For data breaches which resulted (or had the potential to result) in serious / significant harm to a client or individual(s), the s 47(1)(b) will facilitate a post incident review with the appointed Incident Response Team and develop a Post Incident Report (PIR).

The PIR will summarise the breach, assess the effectiveness of Nous' incident management process and identify key learnings from the breach for Nous to apply.

The Post Incident Report will outline any key improvement and remediation actions, which the s 47(1)(b) will assign to relevant employees, subcontractors and/or vendors with an expected implementation date. The report will be distributed to the s 47(1)(b), Nous' Executive Board, members of the Incident Response Team and any other employees who have been assigned an action in the PIR.

6 Training, testing and review

The s 47(1)(b) will provide training to the members of the Incident Response Team for them to be prepared in the event a data breach occurs.

This Data Breach Response Plan will be tested on an annual basis, by the s 47(1)(b) organising a desktop scenario and assessing the preparedness of the members of the Incident Response Team and the effectiveness of the Data Breach Response Plan.

This Data Breach Response Plan will be regularly reviewed to ensure it is up to date and remains relevant.

Policy Owner	s 47(1)(b) [redacted]
Approved by	s 47(1)(b) [redacted]
Last Updated	December 2021
Related Policies	ICT Acceptable Use Policy, Information Classification and Handling Policy, Bring Your Own Device (BYOD) Policy, Information Security Incident Response Plan